US 20020070863A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2002/0070863 A1**

Brooking (43) **Pub. Date: Jun. 13, 2002**

(54) **TAGGING SYSTEM AND METHOD**

(76) Inventor: **Timothy John Brooking**, East Sussex (GB)

Correspondence Address:
SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402 (US)

(21) Appl. No.: **09/978,652**

(22) Filed: **Oct. 16, 2001**

Related U.S. Application Data

(63) Continuation of application No. PCT/GB00/00992, filed on Mar. 16, 2000.

(30) **Foreign Application Priority Data**

Mar. 16, 1999 (GB) 9906037.8

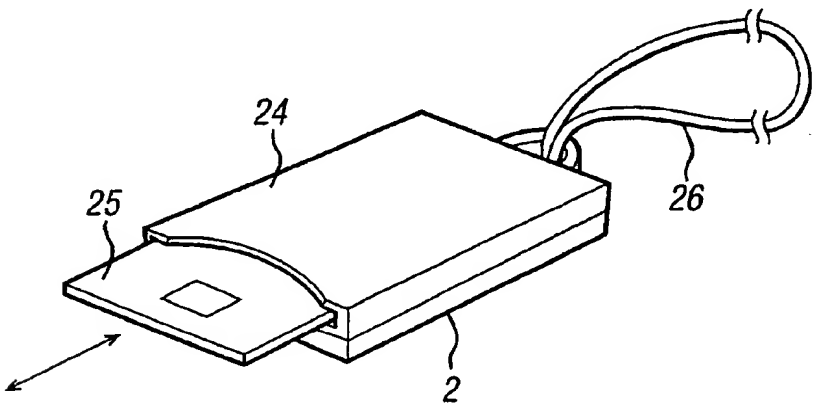
Publication Classification

(51) **Int. Cl.**[7] **G08B 13/14**

(52) **U.S. Cl.** **340/572.1**

(57) **ABSTRACT**

A tagging system for persons or objects comprises tags to be carried by the person or object, each tag transmitting a signal carrying a unique identification code and preferably including a smart card for the purchase of goods and services. A first type of tag detector is arranged at entrances to areas and detects signals from tags passing through the entrances. The detection region of this type of tag detector is limited to the region of the entrances. A database holds information from the respective persons or objects and the unique identification code of the tags being carried by the persons or objects and it receives and stores information on the use of the areas by the person. An entrance processor processes the detected signals to generate an invalid tag signal if a received unique identification code is invalid. A second type of tag detectors is provided for detecting signals from tags in the areas. The detection range of the second type of tag detectors are substantially larger than the detection range of the first type of tag detectors since these are provided for safety reasons or to provide a search and rescue capability. Card readers can be provided at outlets for goods and services in the resort and transactions are recorded in the database to provide further resort management information on spending habits.



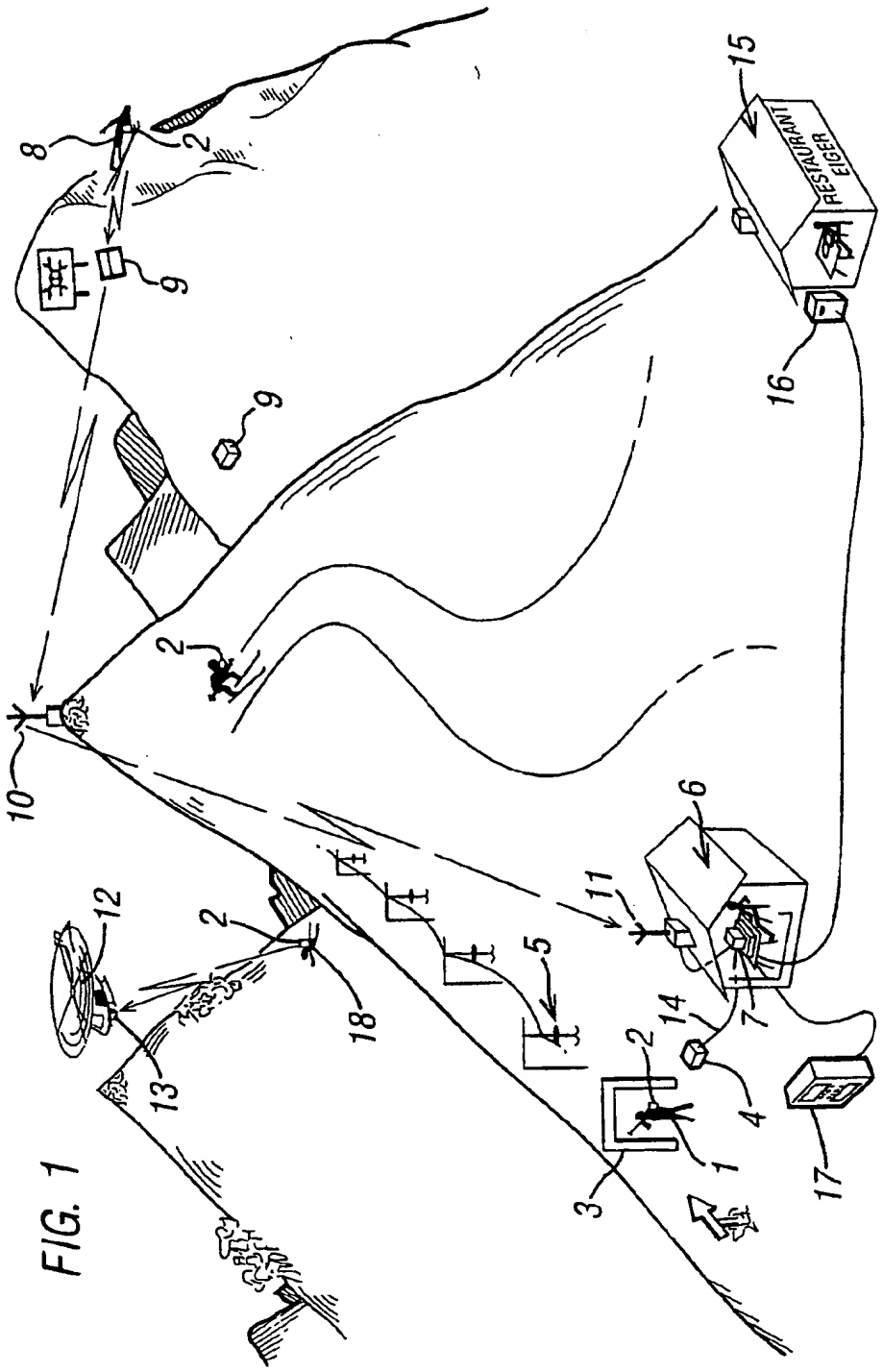


FIG. 1

FIG. 2a

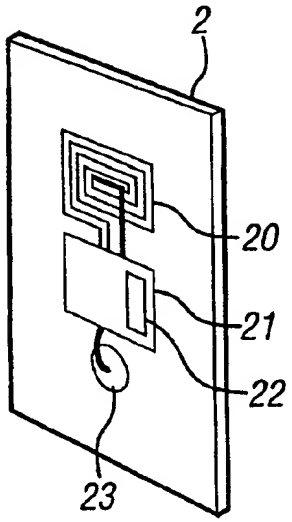


FIG. 2b

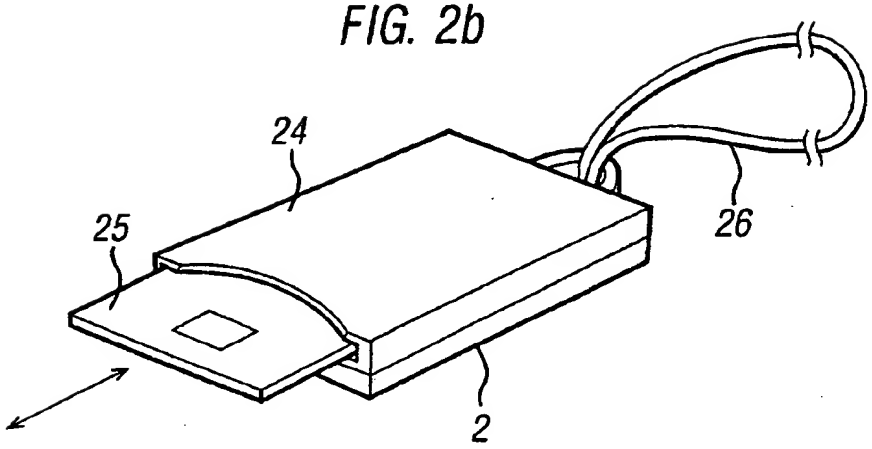


FIG. 3

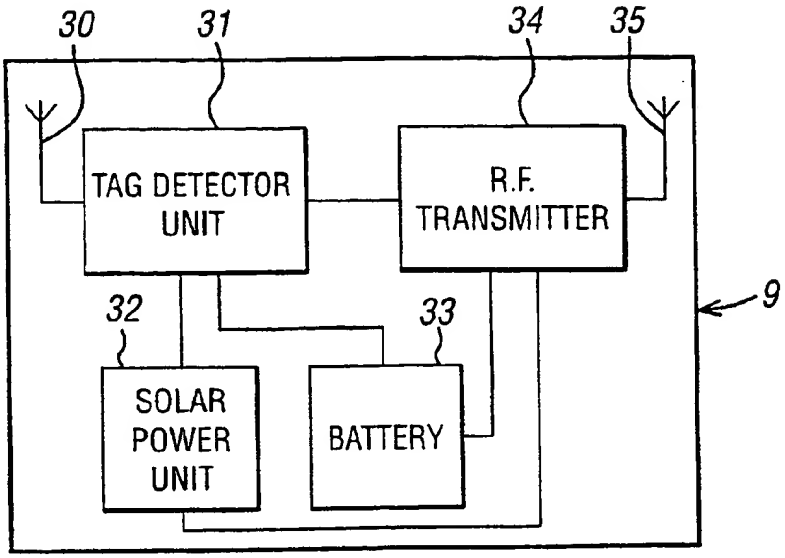

30
31
34
35
TAG DETECTOR UNIT
R.F. TRANSMITTER
9
32
33
SOLAR POWER UNIT
BATTERY

FIG. 4

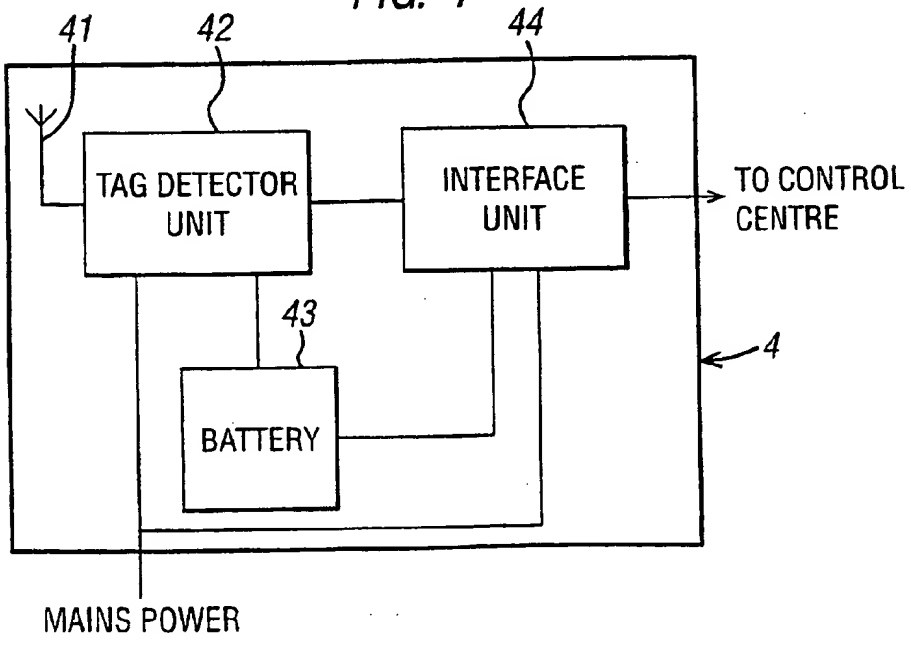
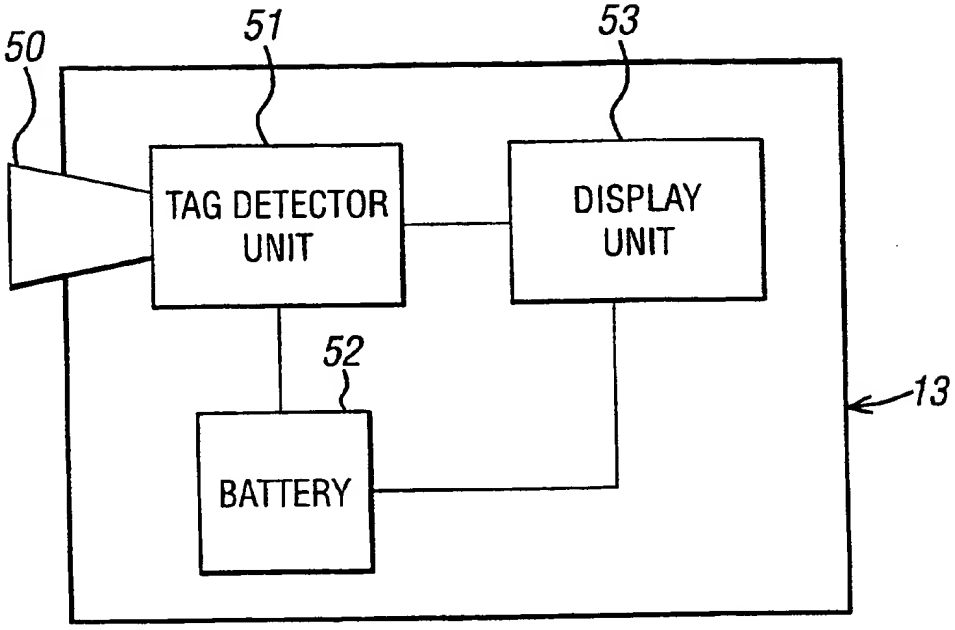

41
42
44
TAG DETECTOR UNIT
INTERFACE UNIT
TO CONTROL CENTRE
43
4
BATTERY
MAINS POWER

FIG. 5



TAGGING SYSTEM AND METHOD

RELATED APPLICATIONS

[0001] This application is a continuation under 35 USC 111(a) of PCT/GB00/00992 filed Mar. 16, 2000 (WO 00155818), which claimed priority from British application Serial No. 99/06037.8, filed Mar. 16, 1999, which applications are incorporated by reference.

FIELD OF THE INVENTION

[0002] The present invention generally relates to a system and method for tagging persons such as skiers, mountaineers or hikers or objects such as boats, cars and airplanes. In particular, one aspect of the present invention relates to an apparatus and method for tagging persons such as skiers, mountaineers or hikers so as to both control access to ski lifts, cable cars etc. giving access to skiing areas or mountains, and to provide a search and rescue capability. The present invention also relates to a resort management system in which a tag stores monetary value information and a processing system links information on persons, locations and monetary value adjustments.

BACKGROUND OF THE INVENTION

[0003] There are in existence methods of enabling search and recovery of personnel lost on mountains or victims of avalanche. Such systems include passive tags sewn into ski wear which may be read by suitable detectors. Such a system is available from RECCO AB. Such a system, however, has a limited range, and it is not known in advance which skiers may have the tagged ski wear.

[0004] It is also known to provide for the automatic accessing of ski lifts and the like using identity cards with photos and bar codes, swipe cards and passive short range tags incorporated within a lift pass.

[0005] There is however, no prior art system which provides a ski lift access control system integrated with an active personal tag which is effective for search and rescue purposes.

SUMMARY OF THE INVENTION

[0006] One aspect of the present invention provides an integrated tagging system which provides both ski lift, cable car access and inter-resort transport control and a personal safety tagging capability which can operate without requiring a transmission licence from the authorities. This aspect of the present invention is designed to use a tag which transmits a signal. As is known tagging system readers (proximity meters) are required to pick up and interpret signals. In this arrangement a first type of detector is provided for access control to detect tags passing through entrances to ski lifts and the like. This is known technology as is used in situations such as accessing the Dartford Tunnel in the UK. Such a type of detector has a limited detection range to limit the region in which tags are detected to only the entrance region of the ski lift and the like. This provides the ski lift access control capability. Thus a skier must carry a ski lift pass which incorporates the tag in order to gain access to the ski lift.

[0007] This aspect of the present invention uses these detectors in an alternative configuration such that they have a much longer range. These may be standard readers as for access control but with range alteration and added antenna configuration considerable reading range is added to the basic reader. These then are provided for security and safety on the skiing areas with the capability of reading the same tag as for accessing the ski lifts. For example, they can be provided in fixed positions in the vicinity of restricted areas to detect persons entering high risk or restricted areas giving resort personnel early warning that skiers may be in danger or in an area that could provoke avalanche risk. Skiers in such areas may be unaware of their position, through adverse weather conditions but specific information on regular offenders, in good conditions and in the knowledge they were illegally "off piste" would be available through the database and necessary action could be taken, such as a stop being put on their lift pass and smart card. Specific knowledge of a skiers whereabouts would reduce search time significantly should he/she be reported lost at anytime since their last recorded reading, be it from a remote or lift reader will be on the database giving time and specific read point geographically. One or more detectors can be used by search and rescue personnel in order to locate skiers, mountaineers or hikers who are lost or incapacitated. Such a type of detector is mobile and can either be hand held or mounted on a vehicle such as a helicopter or snow mobile.

[0008] This aspect of the present invention provides the advantage of an integrated access control system and search and rescue system at low cost since the level of the signals is kept below the level at which a license is required from the authorities. The long range detectors are however sensitive enough to detect tags at a range of 200 to 400 meters, depending on the physical nature and terrain in the area of use.

[0009] In an embodiment of the present invention, the adaptation of the detector for search and rescue use includes using a directional antenna to enable the location and identity of a person carrying the tag to be determined.

[0010] In a preferred embodiment the tag is active and includes a power supply (a battery), a circuit including stored identification code for generating an electromagnetic signal and an antenna for transmitting the signal. Preferably the signal is transmitted as a low frequency radio signal at a level below that which a license is required from the authorities.

[0011] In an alternative embodiment, the tag is passive and responds to an activation signal to transmit the signal. In this embodiment, the first and second tag detectors transmit the activation signal and receive the resultant signal from each tag. In this embodiment, preferably the first tag detectors transmit the activation signal only within the region of a respective entrance and the second tag detectors transmit the activation signal over a substantially larger range.

[0012] In one embodiment the second tag detectors are substantially more sensitive to signals from the tags than the first tag detectors.

[0013] In an embodiment of the present invention, each tag transmits a signal carrying a unique identification code and a database of information on persons and the tags that they are carrying provides an added benefit of being able to not only identify persons if they are unfortunate to have to be located by a search and rescue team, but also it provides

useful management information for a ski resort. The usage of the ski lifts and the like can be logged for each user to identify a pattern of activity. This can be used for management and planning purposes.

[0014] A second aspect of the present invention provides a resort management system in which tags are issued to persons in the resort. Each tag transmits a unique signal to identify the person carrying it and includes a readable storage means for storing monetary value information. Information on the persons who have been issued with tags is collated in a central processor forming an information database. As the person moves around the resort, tags carried by persons are detected in the vicinity of tag detectors. Tag detections are input to the centralized processor to provide information on the location and movement of persons. When a person wishes to purchase goods or services, or top-up the monetary value of the tag, reading means are provided in the resort to adjust the monetary value information carried by the storage means accordingly. Information on the adjustment of the monetary value information is also input to the central processor. Information on the identity and locations of persons and their spending habits is thus formed in the central processor by linking the data obtained from the issuance and detection of tags and the reading of the storage means on the tags.

[0015] Thus when tags are issued to persons using the resort, a great deal of information can be obtained from the person. The tag can be provided to enable the person to gain access to areas of the resort e.g. ski lifts in a ski resort. At the time of issuance of a tag, a person can load the tag with a certain amount of monetary credit to be used for purchases of goods and services throughout the resort. In this way, the tag can be used for gaining access to areas of the resort, and for providing a simple means of purchasing goods and services in the resort.

[0016] In a preferred embodiment, the resort management system uses the tagging system of the first aspect of the present invention to integrate a search and rescue system with a resort management system.

[0017] A convenient form of the tag comprises a tag body housing a transmitter and memory storing the unique tag identification, and a smart card which is removable from the tag body. The smart card contains the monetary value information in a conventional known manner. Identification codes given to the tag and to the smart card can be linked in the central processor for the resort in order to link information on the location and identity of persons and purchases made.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] Embodiments of the present invention will now be described with reference to the accompanying drawings; in which:

[0019] **FIG. 1** is a schematic drawing of the implementation of a tagging system in a ski resort,

[0020] **FIG. 2*a*** is a schematic diagram of one side of a tag;

[0021] **FIG. 2*b*** is a schematic diagram of the other side of the tag;

[0022] **FIG. 3** is a schematic diagram of a tag detector to be provided in the skiing areas;

[0023] **FIG. 4** is a schematic diagram of a tag detector to be provided at the ski lift entrances; and

[0024] **FIG. 5** is a schematic diagram of a tag detector to be used by search and rescue personnel.

DETAILED DESCRIPTION

[0025] Referring to **FIG. 1**, the implementation of a tagging system in a ski resort is illustrated. When a skier wishes to use the ski lifts in order to gain access to the skiing areas, they will be required to purchase a ski pass. The ski pass incorporates the tag and thus when the ski pass is purchased, a tag unique identification number is recorded for the skier together with personal information such as their name, address, contact numbers, place of residence, whether full time or local such as the local chalet, hotel, flat etc. This information can be entered into a database for management purposes.

[0026] As can be seen in **FIG. 1**, when a skier **1** wishes to access the skiing areas, they will necessarily have to carry a ski pass **2** carried about their person. This can be obtained from a kiosk **17** comprising an automatic vending machine. A person enters the required information e.g. name, address etc and enters their credit card details to be issued with a tag and smart card combined. The entered information is transmitted to a central control station **6** to form and store a database.

[0027] As the persons pass through the entrance **3** of the ski lift **5** they pass by tag detectors **4** which are of a first type which have a limited range of detection; the range of detection being limited to the entrance region **3** of the ski lift **5**. Thus, skiers **1** using the ski lift can be detected and logged. The tag detectors **4** are linked via a communication line **14** to a central control station **6**. Within the central control station **6** a computer **7** stores a database of information on the tags and skiers and will thus store ski lift usage information for each skier.

[0028] The tag detector **4** can either include some local processing capability or can refer back to the computer **7** in the central control station **6** in order to perform access control. When the unique identification code of the tag is detected, it is compared with valid codes to determine whether access should be allowed or denied to the skier **1**. Thus for example, if the tag has been reported as being stolen, the validity of the identification code would have been cancelled and thus a skier attempting to use the stolen tag (ski pass) will be denied access to the ski lift. Also, since the ski passes may only be valid for a particular period of time e.g. for the one week stay by the guests at the resort, any attempt to use the ski pass outside this period of validity will result in access to the ski lift being denied.

[0029] All of the information to control access to the ski lift can be stored within the computer **7** within the central control station **6**.

[0030] The tag detector **4** at the entrance **3** to the ski lift **5** is able not just to detect the skiers **1** individually as they pass the entrance but can detect multiple skiers and perform access control rapidly.

[0031] Although in this embodiment a signal line **14** is **20** provided between the tag detector **4** and the computer **7**, a

radio frequency link could be provided instead as illustrated in the embodiment of **FIG. 9** to the control center **6**.

[0032] The tag can also be used for controlling the use of 25 buses to and from the ski lift i.e. it acts as a ticket. In such an arrangement tag detectors such as the tag detectors **4** can be used with an antenna to communicate with the central control station **6**. The tags can thus be used to detect skiers going to and from the ski lift.

[0033] This feature of the embodiment of the present invention thus provides for not only access control to the ski lift and buses but also a monitoring function to allow for the behavior of skiers to be monitored. This can be used f or planning and management purposes.

[0034] Within the resort, there are also provided restaurants and the like to allow persons to buy goods or services. The smart card issued to each person can be used for this purpose. Each smart card is loaded with a certain amount of credit when issued and this can be topped-up when necessary by for example using the kiosk **17**. Thus as shown in **FIG. 1**, at a restaurant **15** there is provided a smart card reader **16** for reading the smart card carried by the tag. The appropriate cost of a meal can be deducted from the value carried by the smart card and this information on the transaction can be transmitted to the central control station **6**. Thus, in this way the computer **7** in the central control station **6** receives not only information on the person received during issuance of the tag and the location information obtained from the tag, but also information on the spending habits of the person. This information can be extremely useful to resort managers for planning and management purposes. The provision of a smart card associated with a tag has the benefit of eliminating the need for separate cash or credit cards in the resort. The smart card and the tag are designed to provide everything a skier should need around the resort by providing access control and means of purchase. From the resort managers point of view, the combined smart card and tag provides the benefit of safety in that locations of skiers can be determined, and security since both the card and tag are linked at the point of issue by associating their unique identification numbers. This protects again fraud in the event of loss.

[0035] At the end of the required use of the card and tag, they can be returned to the machine where a refund on a deposit paid for the tag can be returned together with any remaining credit on the smart card. The tags and cards can then be recycled for further use.

[0036] In the skiing areas, a second type of tag detector **9** can be provided at the boundary of or in a vicinity of regions which the ski resort managers do not wish skiers to access e.g. Of f piste areas, avalanche risk areas, or areas that are simply restricted. The tag detectors **9** have a much greater range than the first type of tag detectors **4** and can be omnidirectional or directional in their detection of tags **2** provided on skiers **8** which enter the restricted areas. Because of the remoteness of the tag detectors **9**, it is usually impractical to provide for land lines to the central control station **6**. Thus the tag detectors **9** are provided with radio frequency transmitters. The transmitters can either have the power to transmit directly to an antenna **11** provided at the central control station **6**, or can be low powered transmitters which are detected by a local antenna **10** which can amplify and relay the signals to the antenna **11** of the central control center **6**.

[0037] In this way the central control station **6** is able to monitor and identify skiers who enter restricted areas. This information can simply be used to warn the skier **8** when they descend that should they violate the restricted area again, sanctions will be taken against them. Alternatively, the violation of the restricted area by the skier **8** could result in the resort managers deciding to take action and intercept the skier. The system provides the information which can allow the resort manager to decide how to act. This information can also be used for giving an indication of the possible location of a skier if they are reported missing. An indication that a skier has passed by certain tag detectors **9** would give an indication of the possible locality of the skier **8**. Of course, the skier may simply have passed by the tag detectors **9** and may have descended from the mountains by some other route.

[0038] If a skier **18** is reported missing, it is possible for search and rescue team to use the tag **2** to be worn by the skier **18** to locate the skier. For example, the search and rescue team can use a helicopter **12** provided with a tag detector **13** of a second type which has a long range capability in order to locate the skier **18**. The tag detector **13** provided in the helicopter **12** has a directional antenna to allow an operator to guide the helicopter **12** in the direction of any signal detected from the tag **2** worn by the skier **18**. The tag detector **13** is even able to detect the skier **18** even when buried under snow due for example to an avalanche. The detector range of the tag detector **13** is anything from 150 to 400 meters. It can be joystick operated over a sweep angle by an operator within the helicopter **12** in order to control both the attitude and azimuth of the antenna.

[0039] Thus the feature of the provision of the long range tag detectors **9** and **13** in this embodiment provides for a safety and security feature within the tagging system and provides a rapid location method for avalanche victims.

[0040] **FIGS. 2*a*** and **2*b*** are schematic diagrams of a tag for use in the system. The tag comprises a ski pass in a tag part **2** and incorporates within the ski pass an antenna **20**, and an electronic circuit **21** connected to the antenna **20** which incorporates a component **22** storing the unique identification code for the tag. The circuit is powered by a small battery **23**. Thus the tag is an active tag which, in order to save battery life periodically such as once every second, transmits a signal at 433.92 MHz and at an output power of 10 mW carrying the unique identification code read from the component **22**. The power of the transmitted signal is below the level at which a license is required. Such tags are commercially available from Advanced Technology Communications Limited for example. The tag can also incorporate an anti-tamper device and a low battery warning device. On one side of the tag part **2** is a smart card holder **24** into which a smart card **25** can be inserted. The tag assembly is also provided with a cord **26** to allow the tag assembly to be hung around a skier's neck. When the smart card **25** is to be used for payment of goods or services, or recharged with monetary credit, it can be removed from the holder **24** and placed in a card reader.

[0041] In this embodiment of the present invention a single **25** (the same) tag is used to provide both access control and a search and rescue capability. It is the detectors for the two capabilities which are different.

[0042] **FIG. 3** is an illustration of the second type of tag detector **9** provided in the vicinity of restricted areas. The

detector **9** includes an antenna **30** for detecting the signals from the tags. The antenna is connected to a tag detector unit **31** for analyzing the signal in order to extract the unique identification code. The unique identification code extracted is then passed to a radio frequency (RF) transmitter **34** which includes an antenna **35** in order to transmit a signal identifying the received unique identification codes either directly to the antenna **11** of the control center **6**, or to the local antenna **10** for retransmission to the antenna **11** of the control center **6**. The tag detector **9** is powered either by a solar power unit **32** or by a battery **33**. The battery **33** is provided for backup when there is not enough output from the solar power unit **32** to power the tag detector **9**. Thus this tag detector **9** does not require either mains power or a direct physical connection with the control center **6** enabling the positioning of these devices in remote areas.

[0043] **FIG. 4** is a schematic diagram of a tag detector **4** provided at the entrance **3** to the ski lift **5**. Such a detector is for example available from Advanced Technology Communications Limited. The tag detector **4** is provided with an antenna **41** connected to a tag detector unit **42** to analyze signals received from the tags in order to extract the unique identification code. This is then passed onto an interface unit **44** which generates a signal for output to the central monitoring station **6**. The tag detector **4** is powered by external mains power and is also provided with a battery backup **43**. Thus, because the tag unit **4** is provided usually in accessible areas, it is provided with mains power and a direct physical connection to the central monitoring station **6**. However, where such facilities are difficult to provide, a unit similar to the tag detector **9** can be provided.

[0044] **FIG. 5** is a schematic diagram of a mobile tag **15** detector **13** for use by the search and rescue personnel. The tag detector **13** is provided with a directional antenna **50**. The antenna **50** can be steerable when the tag detector **13** is provided on a vehicle such as a helicopter. Alternatively, if the tag detector **13** is portable, the antenna **50** can be fixed to allow an operator simply to move the whole device in order to determine the directionality of the received signal i.e. the tag **2**. The signals detected by the antenna **50** are analyzed by a tag detector unit **51** in order to extract the unique identification code and signal. This code is then output to a display unit **53** to display the identification code to an operator. The tag detector **13** is powered by a battery **52**.

[0045] In this unit the mere display of the identification **5** code for a located tag is sufficient since it enables the search and rescue personnel to contact the control center **6** in order to identify the wearer of the tag. This enables the search and rescue personnel to check whether they have located the person who was reported missing. They may actually have located some one who was not reported missing but who nevertheless needs to be rescued. They would thus need to resume the search for the person who was reported missing.

[0046] The tag detectors **9** and **13** are more sensitive than **15** the tag detector **4** and thus have a much greater range enabling their use in the detection of tags in the skiing areas.

[0047] As can be understood from the description of the embodiment of the present invention, one aspect of the present invention provides for a complete ski resort management system which is capable of controlling access to ski lifts, monitoring access to danger areas such as closed runs, off piste areas, avalanche danger areas etc., and enabling an efficient search and rescue operation when skiers are reported missing. This is facilitated by the use of the tag detection system having a limited range for use as a ski lift access control system and of a much greater range for use as a search and rescue system. The preferred system provided is inexpensive since it uses signals which are of low power and below the threshold at which licenses are required from the authorities.

[0048] Although in the specific embodiment described with reference to the drawings, the tag is an active tag having a battery, the present invention is equally applicable to a passive tag wherein the tag detectors are further equipped with a circuit for generating an activation signal which is transmitted to a region in which the tag is to be detected. For the tag detectors **4** for access control, the range of transmission of the activation signal can be restricted to the region around the entrance **3**. For the tag detectors **9** and **13**, the range of the activation signal is much greater in order to provide a greater tag detection range. When the passive tag of this alternative embodiment detects the activation signal, it retransmits or reflects the signal modified by the unique identification code of the tag. This retransmitted or reflected signal can then be detected by the tag detectors.

[0049] Although the embodiments have been described with reference to skiers, the present invention is applicable to any activity where there is a need to control access and to be able to locate persons in an emergency in an area such as on mountains, theme parks and game parks (wild life reserves).

[0050] The tag could incorporate both passive and active chips where the two different types of readers detect either the passive or active port of the tag.

[0051] The application of relatively inexpensive tags to a long range reading capability utilizing helicopter search techniques may be used for search and rescue operations for walkers such as individuals or groups lost on mountains. Although not specifically known by name or number, the aid to their recovery will be greatly enhanced with possible life saving consequences and reduction to the risk of hyperthermia.

[0052] Although the embodiments of the present invention have been described with reference to a system for tagging persons in a resort, the present invention is applicable to the tagging of persons for whatever reason to detect the movement of the persons out of desired regions into undesired regions. For example, the tagging system can be used for tagging prisoners who are released into the community with restrictions on their movements. The tags can be used to monitor the movements and warn of violations of the prisoner's parole.

[0053] Also, the present invention is applicable to the tagging of passengers in an airport by way of tagging the boarding cards. Currently, one of the major problems in airport management is keeping track of passengers who are waiting to board an airplane. Passengers who leave desired regions into undesired regions, e.g. leave the terminal building, can be detected in order to warn the airport managers.

[0054] The personal tagging system is also applicable to search and rescue teams and firemen when carrying out their duties. Once the personnel leave the desired areas and

therefore enter restricted territory, these movements can be detected and a warning provided. Thereafter, the long range tagging system can be used to trace the personnel.

[0055] Although the embodiments of the present invention described hereinabove have been described with reference to a tagging of persons, the present invention is not restricted to this, but is also applicable to the tagging of objects such as boats, cars, airplanes and containers. For example, in a marina application, boats can be tagged and when the boat is in the marina, this can be detected using a low range detector. When a boat leaves the marina without authority, a long range detection system can be used for detecting the location of the boat using the tag. A similar system can be used for detecting the unauthorized movements of cars, airplanes and containers.

[0056] Although the present invention has been described hereinabove with reference to specific embodiments, it will be apparent to a skilled person in the art that modifications can be made without departing from the spirit and scope of the invention.

1. A tagging system for persons or objects, the tagging system comprising:

tags to be carried by the persons or objects, each tag being adapted to transmit a signal carrying an identification code unique to the tag;

at least one first tag detector for arrangement at one or more entrances to areas, and for detecting the identification code carried by the signals from tags passing through the or each respective entrance, the detection region of said at least one first tag detectors being limited to the region of a respective said entrance;

entrance processing means for processing the detected identification codes to generate an invalid tag signal if a received signal is invalid;

at least one second tag detector for detecting the identification code carried by the signal from tags in the areas, the detection range of said at least one second tag detector being substantially larger than said at least one first tag detector; and

database means for holding informnation on respective persons or objects and said codes for tags being carried by respective persons or objects, and for identifying respective persons or objects using identification codes detected by said first and second detectors.

2. A tagging system according to claim 1, wherein said at least one second tag detector includes at least one said second tag detector which is mobile for use for locating lost or incapacitated persons or objects.

3. A tagging system according to claim 1, wherein said at least one second tag detector includes at least one said second tag detector for arrangement in the vicinity of one or more areas restricted for persons or objects; the system including monitoring means for monitoring detections by said at least one second tag detector to warn of any persons or objects in the vicinity of the or each restricted area.

4. A tagging system according to claim 3, wherein each of said at least one second tag detector for arrangement in the vicinity of the or each restricted area includes radio transmitters for transmitting data on detection of tags to said monitoring means, and said monitoring means includes a radio receiver for receiving the data.

5. A tagging system according to claim 1, wherein said at least one second tag detector has a range of at least 150 m.

6. A tagging system according to claim 1, wherein each said tag is active and includes power supply means, a circuit for generating an electromagnetic signal using power from said power supply means, and an antenna for transmitting the electromagnetic signal; and said first and second tag detectors are adapted to receive the transmitted electromagnetic signals from the tags.

7. A tagging system according to claim 6, wherein each said tag is adapted to transmit low frequency radio waves at a level below that at which a licence is required from authorities.

8. A tagging system according to claim 1, wherein each tag is passive and is adapted to respond to an activation signal to transmit said signal; and said first and second tag detectors are adapted to transmit said activation signal and receive said signal from each tag.

9. A tagging system according to claim 8, wherein said at least one first tag detector is adapted to transmit said activation signal only within the region of a respective said entrance, and said at least one second tag detector is adapted to transmit said activation signal over a larger range.

10. A tagging system according to claim 1, wherein said at least one second tag detectors are substantially more sensitive to said signals from said tags than said at least one first tag detectors.

11. A tagging system according to claim 1, wherein each tag includes a smart card in a carrier, said smart card storing monetary value information for purchasing goods and services.

12. A method of tagging persons or objects comprising:

providing each person or object with a tag transmitting a signal carrying an identification code unique to the tag;

detecting identification codes carried by signals from tags passing through one or more entrances to areas using at least one first tag detector which has a detection region limited to the region of the respective entrance;

processing the detected signals to generate an invalid tag signal if a received signal is invalid;

detecting identification codes carried by signals from tags in the areas using at least one second tag detector which has a detection range which is substantially larger than the or each first tag detector; and

identifying respective persons or objects using identification codes detected by said first and second detectors and a database of information on respective persons or objects and said codes for tags being carried by respective persons or objects.

13. A method according to claim 12, wherein at least one of the second tag detectors is mobile and is used for locating and identifying lost or incapacitated persons or objects.

14. A method according to claim 12, wherein at least one of the second tag detectors is arranged in the vicinity of one or more areas restricted for persons or objects and detections of the signals from tags by the or each second tag detector in the vicinity of the or each restricted area is monitored and used to warn of any persons or objects in the vicinity of the or each restricted area.

15. A method according to claim 14, wherein the or each second tag detector arranged in the vicinity of the or each restricted area transmits data on detection of tags to a monitoring station at which the data is received using a radio receiver for performing the monitoring step.

16. A method according to claim 12, wherein the or each second tag detector has a detection range of at least 150 m.

17. A method according to claim 12, wherein each tag is active and actively generates an electromagnetic signal for receipt by said first and second tag detectors.

18. A method according to claim 17, wherein the electromagnetic signal comprises low frequency radio waves at a level below that at which a licence is required from authorities.

19. A method according to claim 12, wherein each tag is passive and responds an activation signal which is transmitted from said first and second tag detectors to transmit said signal.

20. A method according to claim 19, wherein said first tag detector transmits said activation signal only within the region of a respective said entrance and said at least one second tag detector transmits an activation signal over a larger range.

21. A method according to claim 12, wherein the or each second tag detectors are substantially more sensitive to said signal from said tags than the or each first tag detector.

22. A resort management comprising:

tags to be carried by persons in the resort, each tag being adapted to transmit a unique signal to identify the person carrying it and including readable storage means for storing monetary value information;

tag detectors for detecting tags within the vicinity thereof;

information processing means for receiving tag detections to form and store data on the location of persons;

tag issuing means for issuing tags to persons, said tag issuing means being adapted to input information on the persons to said information on the persons to said information processing means; and

storage reading means for reading said storage means of said tags, said storage reading means being adapted to adjust the monetary value information carried by the storage means and to input information on the adjustment of the monetary value information to said information processing means;

wherein said information processing means is adapted to link the data on the location of persons, and the corresponding information on the adjustment of the monetary value information.

23. A resort management system according to claim 22, wherein said tag issuing means comprises at least one automatic vending machine.

24. A resort management system according to claim 22, wherein said readable storage means comprises a smart card carried by said tag.

25. A resort management system according to claim 24, wherein said smart card is removable from said tag.

26. A resort management system according to claim 22, wherein said tags are adapted to transmit a signal carrying an identification code as said unique signal; said tag detectors comprise at least one first tag detector for arrangement at one or more entrances to areas and for detecting the identification code carried by the signals from tags passing through the or each respective entrance, the detection region of said at least one first tag detectors being limited to the region of a respective said entrance, and at least one second tag detector for detecting the identification code carried by the signal from tags in the areas, the detection range of said at least one second tag detector being substantially larger than said at least one first tag detector; and said information processing means includes database means for holding information on respective persons and said codes for tags being carried by respective persons, and for identifying respective persons using identification codes detected by said first and second detectors.

27. A resort management system according to claim 26, wherein said at least one second tag detector includes at least one said second tag detector which is mobile for use for locating lost or incapacitated persons.

28. A resort management system according to claim 26, wherein said at least one second tag detector includes at least one said second tag detector for arrangement in the vicinity of one or more areas restricted for persons; the system including monitoring means for monitoring detections by said at least one second tag detector to warn of any persons in the vicinity of the or each restricted area.

29. A resort management system according to claim 28, wherein each of said at least one second tag detector for arrangement in the vicinity of the or each restricted area includes radio transmitters for transmitting data on detection of tags to said monitoring means, and said monitoring means includes a radio receiver for receiving the data.

30. A resort management system according to claim 26, wherein said at least one second tag detector has a range of at least 150 m.

31. A resort management system according to claim 26, wherein each said tag is active and includes power supply means, a circuit for generating an electromagnetic signal using power from said power supply means, and an antenna for transmitting the electromagnetic signal; and said first and second tag detectors are adapted to receive the transmitted electromagnetic signals from the tags.

32. A resort management system according to claim 31, wherein each said tag is adapted to transmit low frequency radio waves at a level below that at which a licence is required from authorities.

33. A resort management system according to claim 26, wherein each tag is passive and is adapted to respond to an activation signal to transmit said signal; and said first and second tag detectors are adapted to transmit said activation signal and receive said signal from each tag.

34. A resort management system according to claim 33, wherein said at least one first tag detector is adapted to transmit said activation signal only within the region of a respective said entrance, and said at least one second tag detector is adapted to transmit said activation signal over a larger range.

35. A resort management system according to claim 26, wherein said at least one second tag detectors are substantially more sensitive to said signals from said tags than said at least one first tag detectors.

36. A resort management method comprising:

issuing tags to be carried by persons, each tag being adapted to transmit a unique signal to identify the person carrying it and including readable storage means for storing monetary value information;

inputting information on the persons issued with tags to information processing means;

detecting tags in the vicinity of tag detection in the resort;

inputting tag detection information to said information processing means to form and store data on the locations of persons;

reading said storage means of said tags to adjust the monetary value information carried by the storage means;

inputting information on the adjustment of the monetary value information to said information processing means; and

linking the data on the persons, the locations of the persons and the corresponding information on the adjustment of the monetary value information.

37. A resort management method according to claim 36, wherein each said tag transmits a signal carrying an identification code unique to the tag; the step of detecting tags comprises detecting identification codes carried by signals from tags passing through one or more entrances to areas using at least one first tag detector which has a detection region limited to the region of the respective entrance, and detecting identification codes carried by signals from tags in the areas using at least one second tag detector which has a detection range which is substantially larger than the or each first tag detector; and the identifying means identifies respective persons using identification codes detected by said first and second detectors and a database of information on respective persons and said codes for tags being carried by respective persons.

38. A resort management method according to claim 37, wherein at least one of the second tag detectors is mobile and is used for locating and identifying lost or incapacitated persons.

39. A resort management method according to claim 37, wherein at least one of the second tag detectors is arranged in the vicinity of one or more areas restricted for persons and detections of the signals from tags by the or each second tag detector in the vicinity of the or each restricted area is monitored and used to warn of any persons in the vicinity of the or each restricted area.

40. A resort management method according to claim 39, wherein the or each second tag detector arranged in the vicinity of the or each restricted area transmits data on detection of tags to a monitoring station at which the data is received using a radio receiver for performing the monitoring step.

41. A resort management method according to claim 37, wherein the or each second tag detector has a detection range of at least 150 m.

42. A resort management method according to claim 37, wherein each tag is active and actively generates an electromagnetic signal for receipt by said first and second tag detectors.

43. A resort management method according to claim 42, wherein the electromagnetic signal comprises low frequency radio waves at a level below that at which a licence is required from authorities.

44. A resort management method according to claim 37, wherein each tag is passive and responds an activation signal which is transmitted from said first and second tag detectors to transmit said signal.

45. A resort management method according to claim 44, wherein said first tag detector transmits said activation signal only within the region of a respective said entrance and said at least one second tag detector transmits an activation signal over a larger range.

46. A resort management method according to claim 37, wherein the or each second tag detector is substantially more sensitive to said signal from said tags than the or each first tag detector.

47. A tagging system for persons or objects, the tagging system comprising:

tags to be carried by the persons or objects, each tag being adapted to transmit a signal carrying an identification code unique to the tag;

at least one first tag detector for arrangement in the vicinity of one or more areas and for detecting identification codes carried by signals from tags in the vicinity of said areas, the detection region of said at least one first tag detectors being limited to said areas;

processing means for processing the detected signals to determine when persons or objects are in the vicinity of the area;

at least one second tag detector for detecting the identification codes carried by signals from tags away from said areas, the detection range of said at least one second tag detector being substantially larger than said at least one first tag detector; and

database means for holding information on respective persons or objects and said codes for tags being carried by respective persons or objects, and for identifying respective persons or objects using identification codes detected by said first and second detectors.

* * * * *

US005548106A

United States Patent [19]

Liang et al.

[11] Patent Number: 5,548,106

[45] Date of Patent: Aug. 20, 1996

[54] METHODS AND APPARATUS FOR AUTHENTICATING DATA STORAGE ARTICLES

[75] Inventors: **Louis H. Liang**, Los Altos, Calif.; **Daniel A. Marinello**, Burlington, Ky.; **William J. Ryan**, Underhill, Vt.

[73] Assignee: **Angstrom Technologies, Inc.**, Florence, Ky.

[21] Appl. No.: **298,387**

[22] Filed: **Aug. 30, 1994**

[51] **Int. Cl.**[6] **G06K 7/10**; G06K 7/14

[52] **U.S. Cl.** **235/454**; 235/468; 235/472; 235/491

[58] **Field of Search** 235/454, 472, 235/491, 468

[56] **References Cited**

U.S. PATENT DOCUMENTS

Re. 31,302	7/1983	Stambler .	
D. 297,642	9/1988	Van der Tuuk	D14/107
D. 298,536	11/1988	Brefka	D14/105
D. 340,036	10/1993	Connors et al.	D14/105
D. 340,919	11/1993	Lee	D14/105
D. 347,213	5/1994	Bianco	D21/38
D. 348,052	6/1994	Fennell	D14/105
2,593,206	4/1952	Short .	
2,609,928	9/1952	Doust .	
3,105,908	10/1963	Burkhardt et al. .	
3,305,089	2/1967	Fraenkel .	
3,430,200	2/1969	Barney .	
3,463,906	8/1969	Chiang .	
3,473,027	10/1969	Freeman et al. .	
3,492,478	1/1970	Smith .	
3,573,731	4/1971	Schwend .	
3,582,623	6/1971	Rothery et al. .	
3,628,016	12/1971	Berler .	
3,662,181	5/1972	Hercher et al. .	

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

WO92/08211 5/1992 WIPO .

OTHER PUBLICATIONS

Fant et al. "Infra Red Transparent Credit Card" IBM Technical Disclosure Bulletin, vol. 9, No. 7 (Dec. 1966) p. 870.

Ruth Coxeter, Ed.:"How Sour Notes Can Fight Credit Card Fraud" Business Week (Apr. 4, 1994) p. 95.

Bill Peay "In The Cards/Art Guard User" Moneycard Collector vol. 1 No. 3 (Nov. 1994) pp. 14–15.

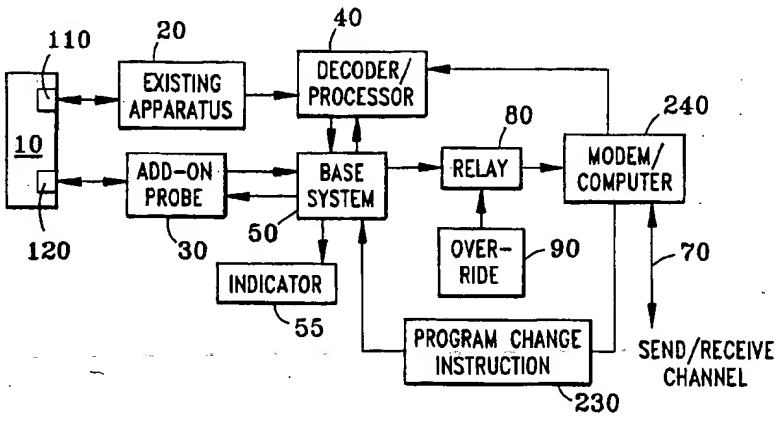
Primary Examiner—Harold Pitts

Attorney, Agent, or Firm—Theodore R. Touw

[57] **ABSTRACT**

Accessory apparatus for authenticating articles is used in conjunction with existing readers or scanners of articles bearing stored data, such as credit cards or identification cards. The accessory apparatus is disposed before, after, on, under, inside, or adjacent to existing reader apparatus, to have a view of the article whose data is to be read. Information in addition to the stored data is coded on the article in non-visible indicia and is detected by the accessory authenticating apparatus. This coded additional information may be related to identification data stored in the article by the article's normal storage mechanism, such as a magnetic stripe or an embedded memory IC chip. The additional information may be coded in various combinations of predetermined characteristics of light emitted by the article to be authenticated when the article is irradiated with non-visible light from the accessory apparatus. The code combinations are preferably complex combinations of the various radiation characteristics. The article is irradiated at a high enough frequency (above 10,000 Hz modulation) for rapid determination of authenticity, and for reading and decoding standard bar codes. Visible and/or audible indicators alert a user when the authentication process detects an invalid card. With certain arrangements, an invalid card may be blocked from being read by the existing reader or scanner. The accessory apparatus may be connected to interrupt the normal communication channel of the existing reader or scanner with which it is used, when an article fails to be authenticated. The accessory apparatus may be used as an adjunct to existing readers or scanners of information on such cards or other articles, to perform authentication functions without replacing or obsoleting such existing readers or scanners.

46 Claims, 6 Drawing Sheets



U.S. PATENT DOCUMENTS

3,663,813	5/1972	Shaw .	
3,691,350	9/1972	Kuhns et al. .	
3,751,640	8/1973	Daigle et al. .	
3,764,978	10/1973	Tyburski et al. .	
3,767,305	10/1973	Craven .	
3,924,105	12/1975	Gassino et al. .	
4,202,491	5/1980	Suzuki .	
4,275,299	6/1981	Favre .	
4,359,633	11/1982	Bianco .	
4,436,991	3/1984	Albert et al.	235/468
4,500,777	2/1985	Drexler	235/487
4,538,290	8/1985	Nakamura	378/44
4,642,526	2/1987	Hopkins	315/244
4,678,898	7/1987	Rudland	235/468
4,694,148	9/1987	Diekemper et al.	235/468
4,711,996	12/1987	Drexler	235/468
4,760,247	7/1988	Keane et al.	235/454
4,795,894	1/1989	Sugimoto et al.	235/468
4,853,524	8/1989	Yamaguchi et al.	235/468
4,873,427	10/1989	Virdia	235/492
4,882,195	11/1989	Butland	427/1
4,889 365	12/1989	Chouinard	283/70
4,889,367	12/1989	Miller	283/88
4,897,531	1/1990	Someya et al.	235/440
4,908,516	3/1990	West	250/556
5,015,830	5/1991	Masuzawa et al.	235/441
5,030,832	7/1991	Williams	250/458.1
5,064,221	11/1991	Miehe et al.	283/67
5,095,194	3/1992	Barbanell	235/379
5,105,073	4/1992	Kovach et al.	235/482
5,173,597	12/1992	Anglin	235/483
5,180,901	1/1993	Hiramatsu	235/380
5,180,902	1/1993	Schick et al.	235/380
5,180,905	1/1993	Chen et al.	235/483
5,196,682	3/1993	Englehardt	235/454
5,210,411	5/1993	Oshima et al.	250/271
5,231,276	7/1993	Yoshihara	235/454
5,254,860	10/1993	Yeh et al.	250/566
5,260,552	11/1993	Colbert et al.	235/482
5,266,789	11/1993	Anglin et al.	235/483
5,270,526	12/1993	Yoshihara	235/487
5,284,364	2/1994	Jain	283/87
5,291,006	3/1994	Nishiguma et al.	235/454
5,291,027	3/1994	Kita et al.	250/566
5,304,789	4/1994	Lob et al.	235/487
5,306,899	4/1994	Marom et al.	235/382
5,311,594	5/1994	Penzias	380/23
5,317,138	5/1994	Togawa	235/454
5,321,243	6/1994	Groves et al.	235/449
5,324,926	6/1994	Huriguchi et al.	235/494
5,386,106	1/1995	Kumar	235/472

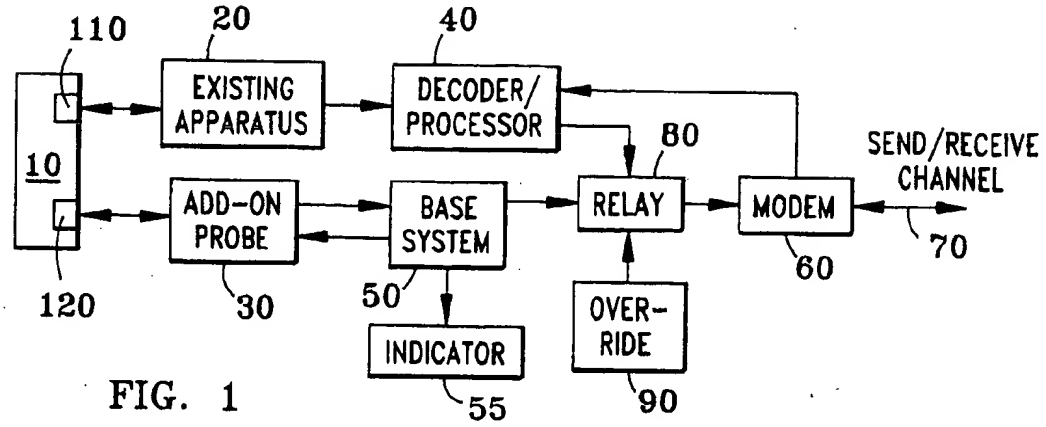


FIG. 1

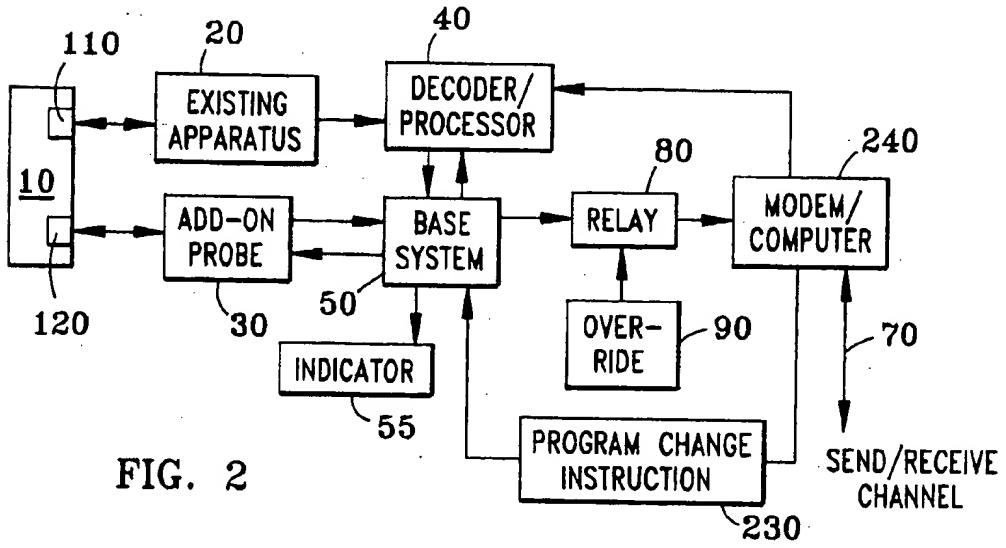


FIG. 2

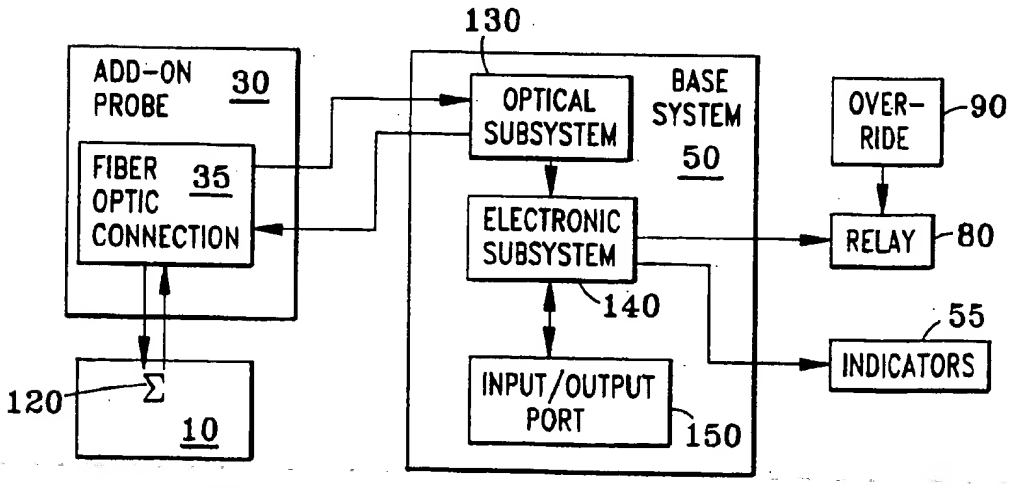


FIG. 3

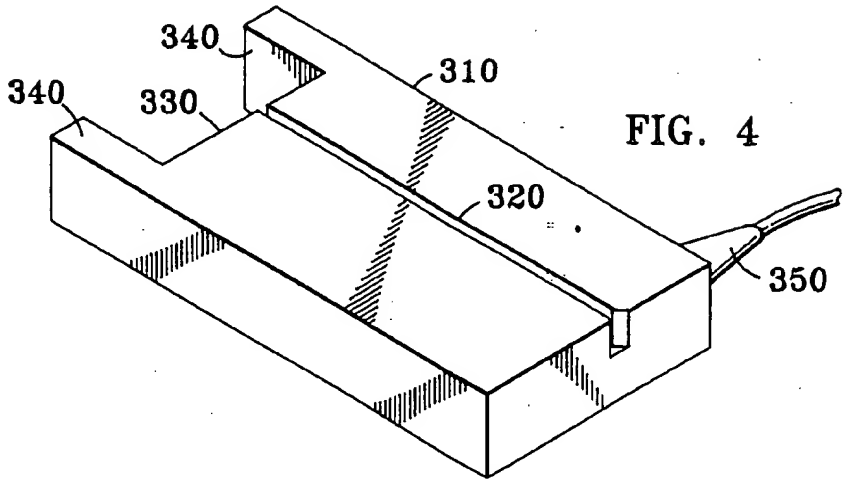


FIG. 4

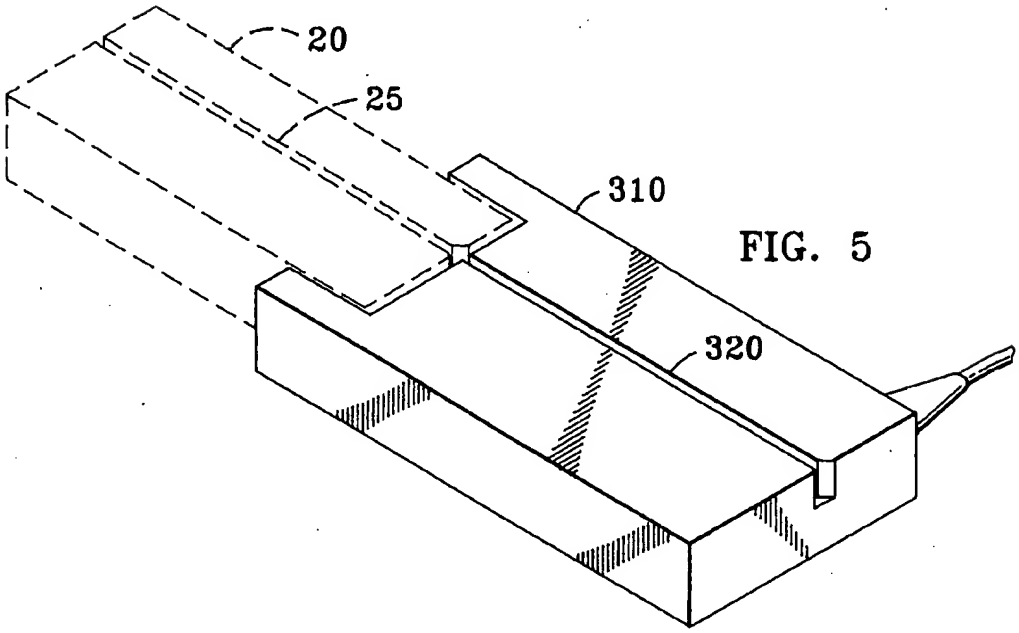


FIG. 5

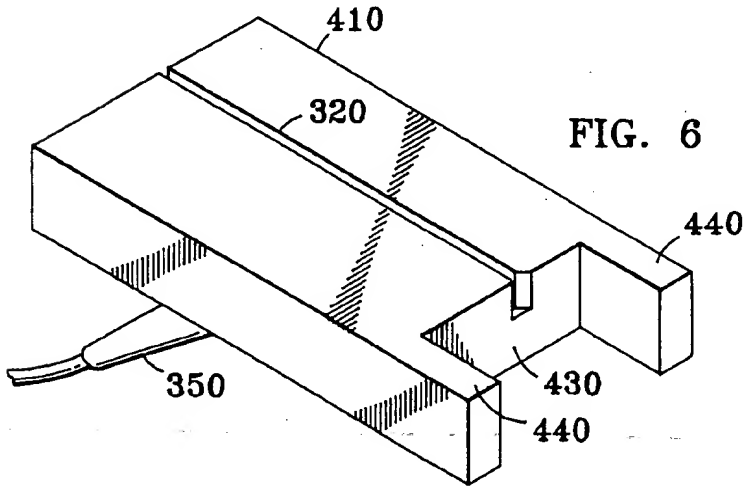


FIG. 6

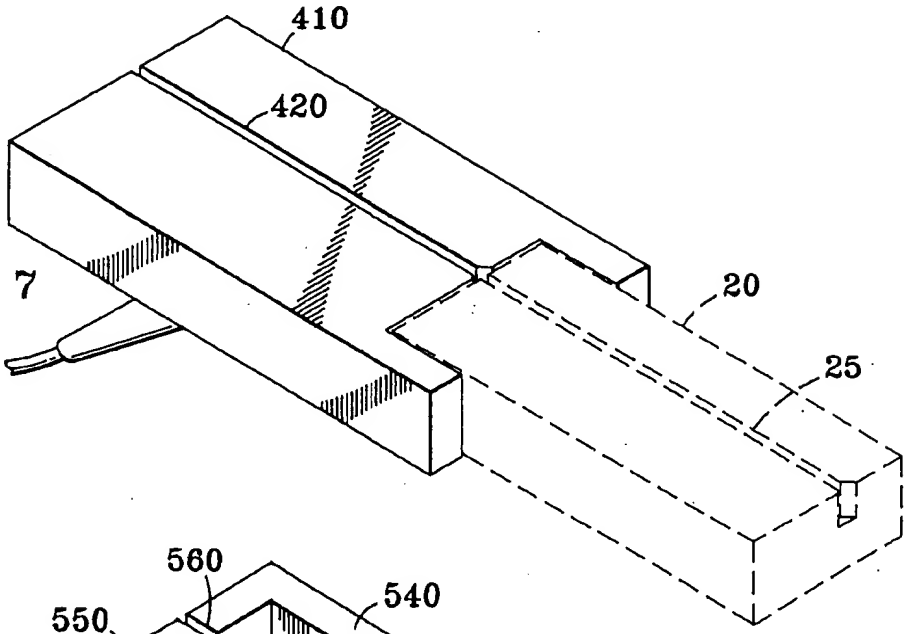


FIG. 7

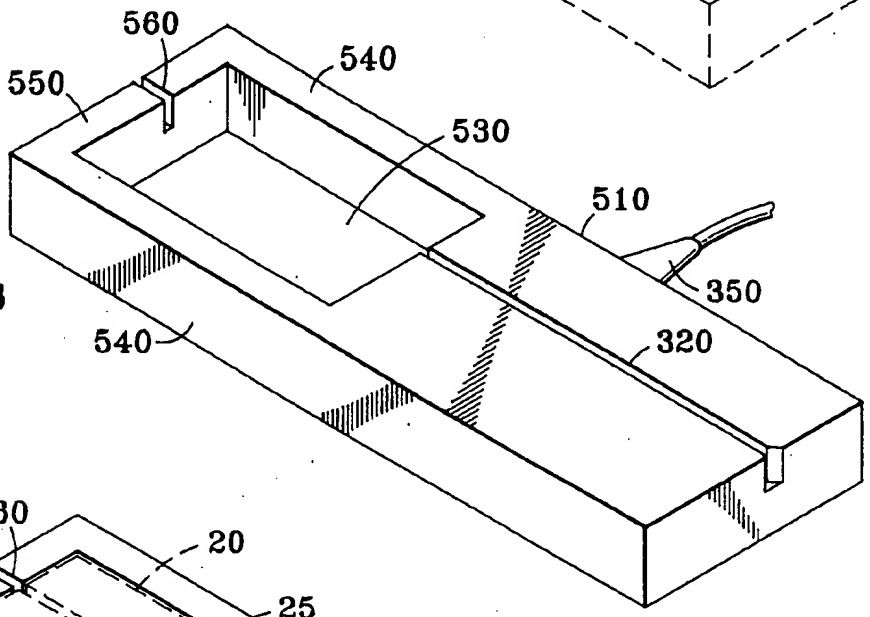


FIG. 8

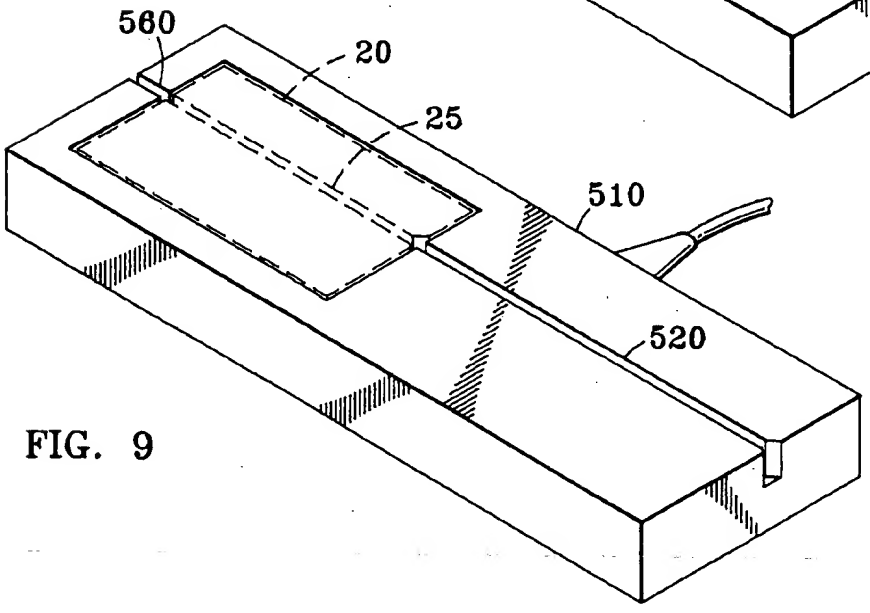


FIG. 9

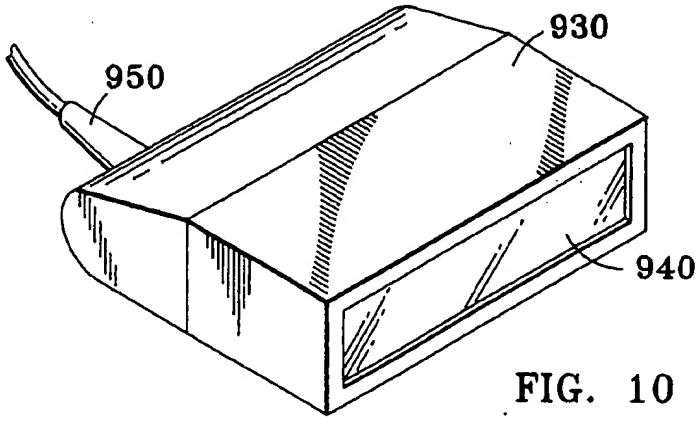


FIG. 10

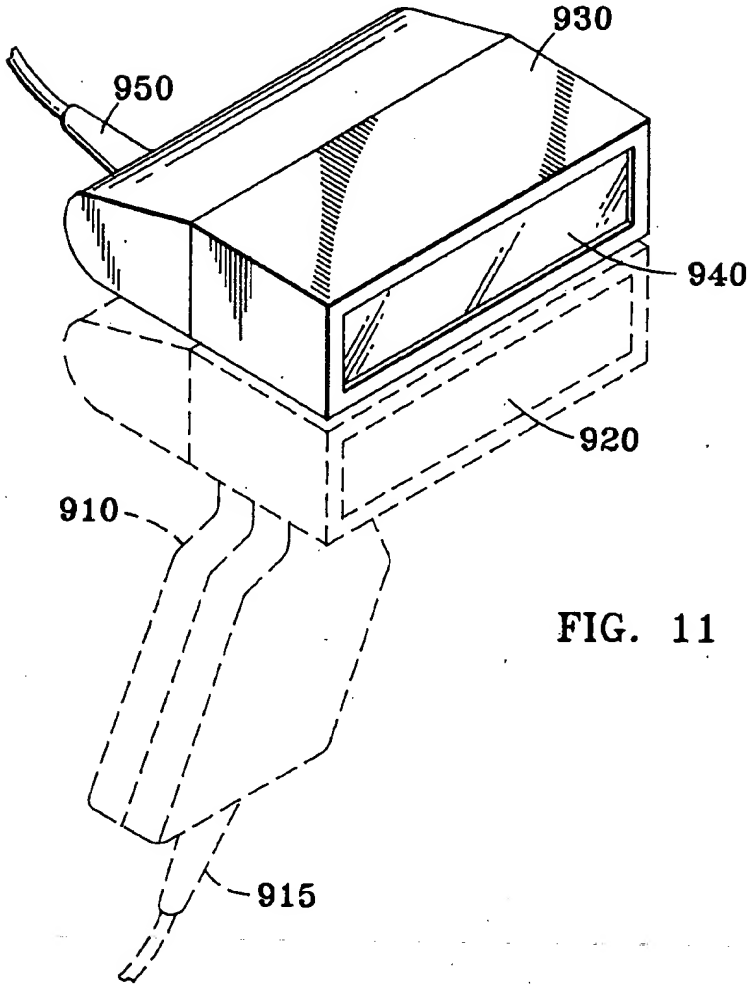


FIG. 11

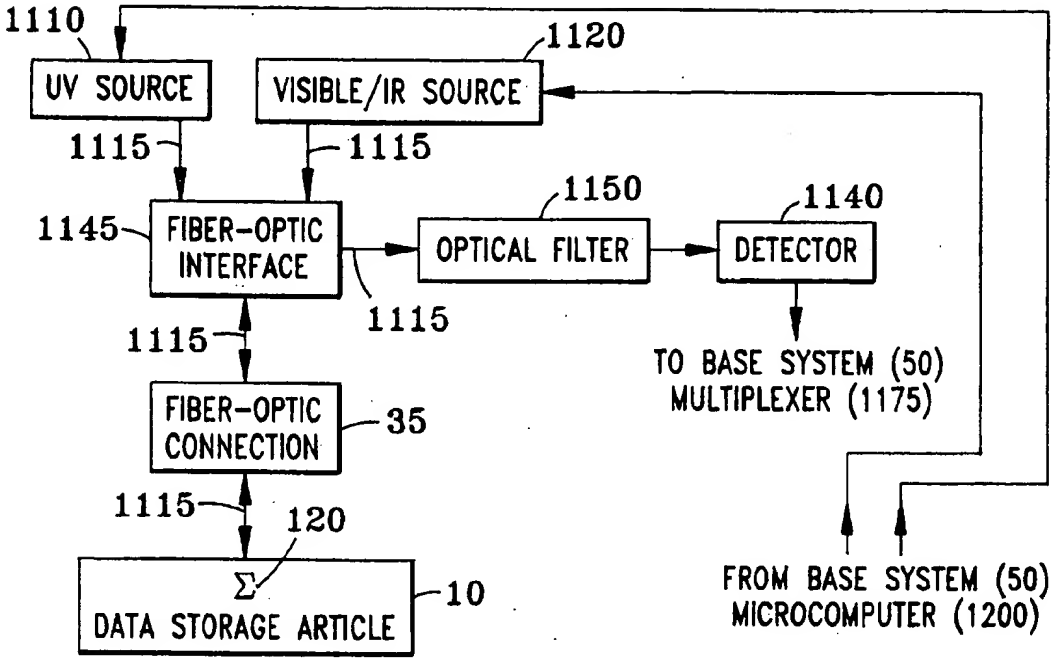

1110
UV SOURCE
1120
VISIBLE/IR SOURCE
1115
1115
1145
FIBER-OPTIC INTERFACE
1150
OPTICAL FILTER
1140
DETECTOR
1115
1115
TO BASE SYSTEM (50)
MULTIPLEXER (1175)
FIBER-OPTIC CONNECTION
35
1115
120
Σ
DATA STORAGE ARTICLE
10
FROM BASE SYSTEM (50)
MICROCOMPUTER (1200)

FIG. 12

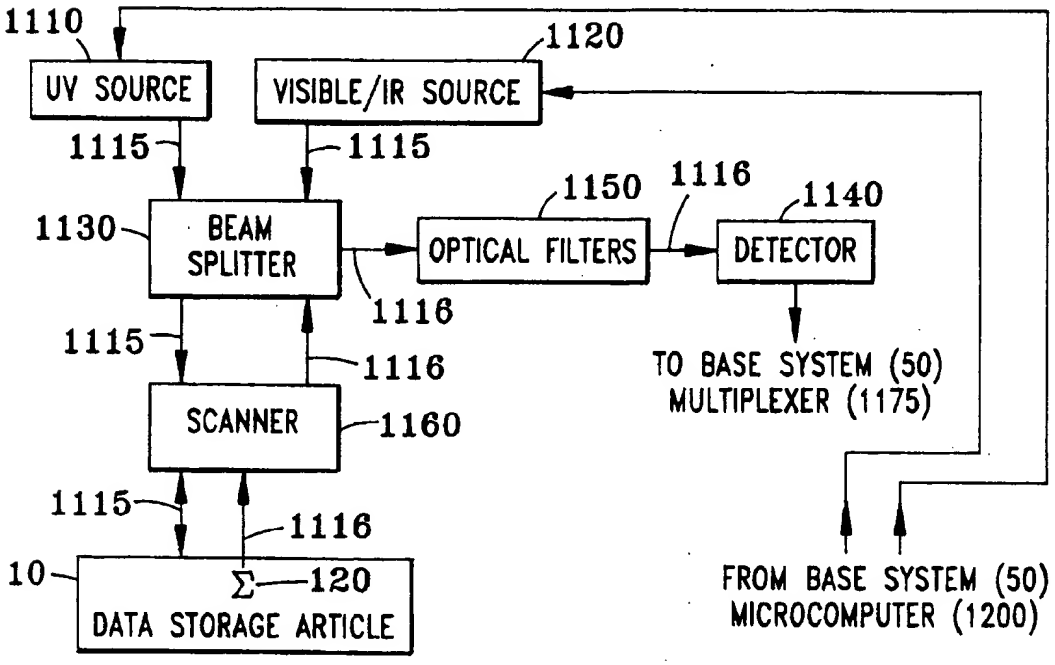

1110
UV SOURCE
1120
VISIBLE/IR SOURCE
1115
1115
1130
BEAM SPLITTER
1150
1116
OPTICAL FILTERS
1140
DETECTOR
1116
1115
1116
TO BASE SYSTEM (50)
MULTIPLEXER (1175)
SCANNER
1160
1115
1116
10
Σ
120
DATA STORAGE ARTICLE
FROM BASE SYSTEM (50)
MICROCOMPUTER (1200)

FIG. 13

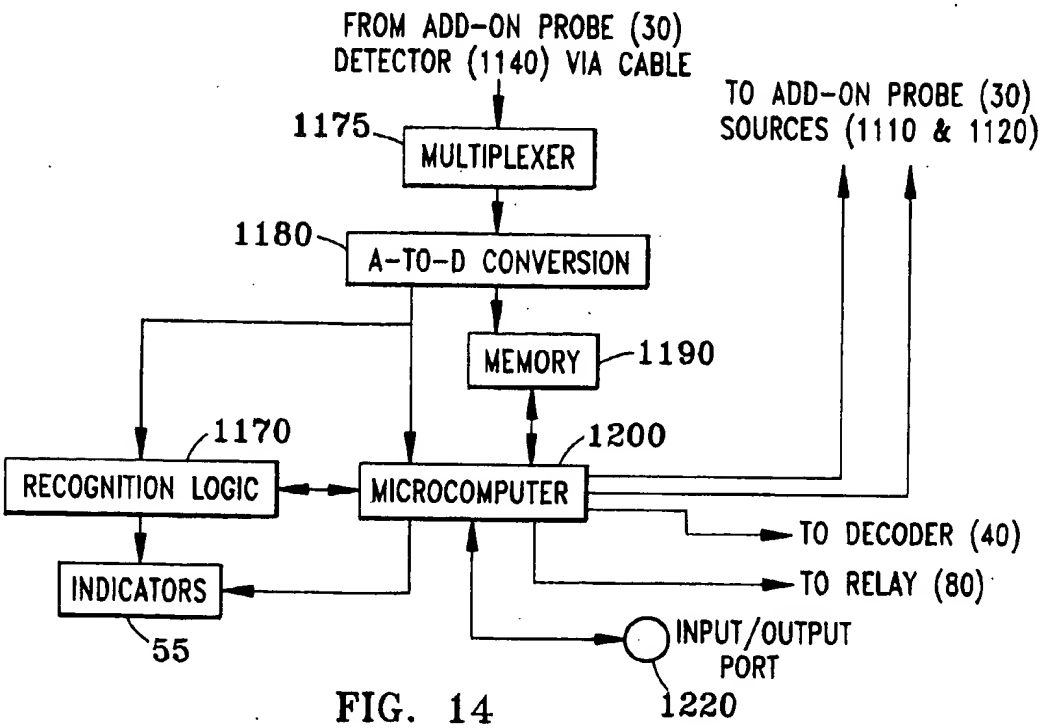


FIG. 14

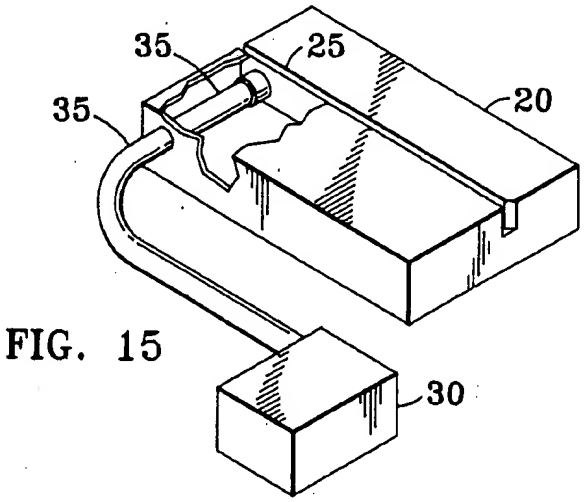


FIG. 15

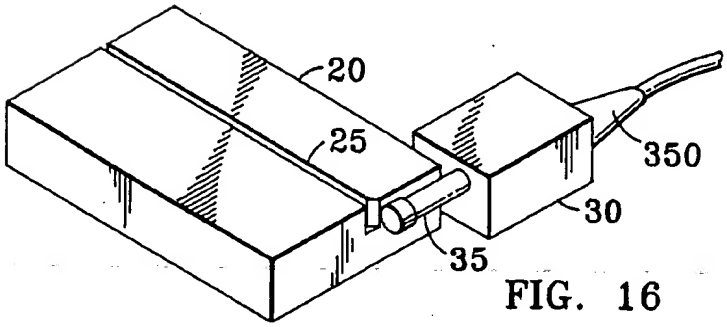


FIG. 16

METHODS AND APPARATUS FOR AUTHENTICATING DATA STORAGE ARTICLES

FIELD OF THE INVENTION

This invention relates to methods and apparatus for authenticating data storage articles such as credit cards bearing recorded information. It relates particularly to auxiliary methods and to accessory apparatus that may be used as adjuncts to existing readers or scanners of information on such cards or other articles, to perform authentication functions without replacing or obsoleting such existing readers or scanners.

BACKGROUND OF THE INVENTION

With ever-increasing use of cards of various types for carrying information, for identification, and for authorizing financial transactions, there has also been an increased incidence of fraud and forgery in which counterfeit cards are used. The annual cost of credit-card forgery alone has been reported in the hundreds of millions of dollars ("Business Week" Apr. 4, 1994, page 95), despite many attempts to prevent fraud by various means to authenticate credit cards. Cards other than credit cards are used to carry coded information about the identity of individuals, their licenses to drive automobiles or to operate other equipment, their authorization for access to restricted facilities, their eligibility for various services such as medical care, etc. Such "credit card" size data storage articles include identification and security cards (driver's license, employee ID cards, badges, access control cards, immigration cards, etc.), financial and transaction cards (credit cards, debit cards, ATM cards, phone cards, subway cards, etc.), data cards (medical information, insurance and benefit information cards, car registration, etc.), telecommunication technician test cards, smart cards, computer memory cards, etc. Such cards may be subject to the same methods of counterfeiting as those used for credit cards. With technical advances and easy access to technologies such as personal computers, graphic software, image scanners, laminating equipment, credit card impact printers, instant-print cameras, and other card-making materials and equipment, a counterfeiter can easily forge such cards including most visible security features employed on them. Examples of such visible security features which can be replicated by counterfeiters are patterned backgrounds, holograms, pictures, and fingerprints. Therefore, there is a need to provide additional security features that cannot be duplicated with technologies based on visible features, and a need to provide automatic authentication that does not rely on human subjective judgment.

The current installed base of credit card readers in the U.S. and Canada alone is estimated at over 40 million units according to the American Bankers Association. World-wide installations of all types of card readers easily exceed billions of dollars in equipment value. Therefore, it is highly desirable to provide an add-on device to the existing readers that can detect invisible security features.

Thus there is an important and continuing need to prevent fraud based on counterfeit data storage articles, particularly data storage articles in the form of a card. At the same time, business enterprises and especially retail establishments, have invested in millions of card readers and/or scanners. It is highly desirable to have methods and apparatus for authentication of cards that would not require businesses to replace their existing card readers or existing scanners with a new type of authenticating reader or scanner.

NOTATIONS AND NOMENCLATURE

In this specification the expressions "non-visible light" and "non-visible radiation" will refer to light radiation with a peak wavelength outside the spectral range normally visible to the human eye. Such "non-visible light" may also include a broad enough wavelength range that a minor portion of its spectral composition may also fall within the boundaries of the visible spectrum. The visible spectrum extends from about 400 nanometers to about 700 nanometers. An example of a source of non-visible light in this sense is a high-pressure mercury lamp.

"Data storage card" and "data storage article" both refer to articles in which information is stored. Such articles need not necessarily have the form of a card, but can have other forms such as tags, badges, tapes, disks, tickets, checks, certificates, and coupons. Among those data storage articles in the form of a card or tag, the information readable by an existing reading device may be encoded in a variety of ways including magnetic stripes, characters printed in magnetic ink, characters readable by OCR equipment, embossed characters, visible or invisible bar codes, RF transponder characteristics, images, holograms, and others. The information stored in articles of other forms may be stored by any of the physical mechanisms employed for such articles.

DESCRIPTION OF THE RELATED ART

Many methods have been described for preventing counterfeiting or fraudulent use of cards bearing stored data. A few examples of these are listed here. Fant et al. described an infrared transparent credit card ("Infrared Transparent Credit Card," IBM Tech. Discl. Bulletin, Vol. 9, No. 7, December 1966, p. 870). U.S. Pat. No. 3,585,593 (Roberts, 1971) disclosed a device for identifying credit cards using coded holes punched in the card in accordance with a code given only to the legal owner of the card. Greenway (U.S. Pat. No. 4,119,361, 1978) disclosed a multilayer identification card containing fine-structure optical markings readable with infrared light through a protective layer which is opaque to lesser wavelengths. U.S. Pat. No. 4,202,491 (Suzuki, 1980) describes a data card containing data recorded with a fluorescent material that emits infrared rays when excited by infrared rays. U.S. Pat. No. 4,538,059 (Rudland, 1985) discloses an identification card with concealed coding made by infrared transparent windows of two widths providing binary coding readable by infrared radiation through material opaque to visible light. U.S. Pat. No. 4,694,148 (Diekemper et al., 1987) shows an access card having coded markings which appear in an infrared receiver under infrared radiation, having a photosensitive layer, and having a surface layer not transparent to visible light. U.S. Pat. No. 4,873,427 (Virdia, 1989) uses a plastic card with an integrated memory circuit and with infrared-transparent layers over identification codes readable by transmission of infrared light.

In U.S. Pat. No. 4,897,531 (1990), Someya et al. disclose a data identifying system that reads a data card magnetic stripe, and reads an optical ROM card containing data regarding invalid cards to determine whether the data card is invalid. U.S. Pat. No. 4,908,516 (West, 1990) discloses apparatus and a process that irradiates an article such as a card having magnetic data storage with predetermined radiation and determines whether detected radiation has pre-

scribed spectral characteristics. West's apparatus controls an integral magnetic detecting head according to the result of radiation detection. U.S. Pat. No. 4,972,476 (Nathans, 1990) discloses an ID card bearing a scrambled facial image. U.S. Pat. No. 5,095,194 (Barbanell, 1992) discloses a holographic credit card that stores a unique identification such as a fingerprint of the authorized user in the form of a hologram. U.S. Pat. No. 5,104,149 (Hoppe, 1992) has a security print covering the surroundings of a signature field and extending continuously across the signature field as well. U.S. Pat. No. 5,151,582 (Fujioka, 1992) uses light-emitting elements and image sensors of reflected light to read and check the embossed information on a card. Gross et al., (PCT Publication No. WO 92/08211, 1992) describe an access control device using a number of machine-readable data substrates bearing access authorizations in coded form, but readable only by different reading devices. U.S. Pat. No. 5,180,901 (Hiramatsu, 1993) discloses a pressure sensor and an authenticity sensor arranged on the surface of an IC card. U.S. Pat. No. 5,180,902 (Schick et al., 1993) shows a self-verifying transaction card having a self-contained keyboard or keypad. U.S. Pat. No. 5,202,930 (Livshitz et al., 1993) uses correlation function analysis on the dynamics of a sample and reference signatures. U.S. Pat. No. 5,216,233 (Kassens, 1993) uses an RF identification label alone or with any of a series of scanner modules for data capture. U.S. Pat. Nos. 5,270,526 and 5,321,276 (Yoshihara, 1993) show card-type recording media having plural types of inks which normally exhibit the same color visually, but have different optical characteristics under a predetermined condition provided in blocks in a desired pattern. U.S. Pat. No. 5,239,166 (Graves, 1993) uses secure data interchange between an intelligent card and a terminal, and uses erasure of data upon an invalid response. U.S. Pat. No. 5,305,383 (Guillou et al., 1994) uses a system of numbered tokens with a chip card for electronic payment. U.S. Pat. No. 5,311,594 (Penzias, 1994) describes a system using pre-stored authentication information, randomly requested of a card user at each transaction. U.S. Pat. No. 5,317,137 (Wilkins, 1994) discloses a system which magnetically writes a security code simultaneously with magnetic reading of a card, and validates or re-validates the card only if the same security code is present before completion of a transaction. U.S. Pat. No. 5,334,823 (Noblett, Jr. et al., 1994) discloses a system and methods for operating a data card terminal which include an embossed character reader, a magnetic stripe reader, and a signature-capture printer which digitizes and compresses signals corresponding to the signature of a card-holder.

Ronald S. Indeck et al. describe a method of detecting and analyzing a "signature" pattern of the minute magnetic particles of which a magnetic stripe is composed, which can be used for authenticating cards [Ruth Coxeter, ed. "How Sour Notes Can Fight Credit Card Fraud" Business Week, Apr. 4, 1994, p. 95; G. Mian et al. "Noise Correlation of Magnetic Thin Film Media" Japanese Journal of Applied Physics, Part 2 (Letters) Vol. 30. No. 8B, pp. L1483–L1485 (Aug. 15, 1991); and J. R. Hoinville et al. "Spatial Noise Phenomena of Longitudinal Magnetic Recording Media" IEEE Transactions on Magnetics, Vol. 28 No. 6, pp. 3398–3406, November 1992].

Various technologies such as surface acoustic wave (SAW) technology, encrypted radio-frequency-activated circuits, and encrypted integrated circuits have been proposed as counterfeit protection features for the above-mentioned data storage articles. These offer many advantages, such as high memory capacity for data, field programmability, extended detection range, no requirement for "line of sight" communication, and an ability to provide personalized codes.

Many inventions have been made using light-emitting materials and corresponding dedicated detection systems. U.S. Pat. No. 4,642,526 (Hopkins, 1987) discloses an object recognition system using modulated ultraviolet light produced by a self-modulated lamp. U.S. Pat. No. 4,889,365 (Chouinard, 1989) discloses a counterfeit resistant label made by applying a selected code word as a series of marks in several locations on the label (using ink sensitive to light in the non-visible spectrum), and by masking the ink visibility at all of the locations. U.S. Pat. No. 4,889,367 (Miller 1989) has a multi-readable information system, using bar codes in an ink readable by light of a first wavelength and using human-readable symbols printed on the same area with humanly visible ink.

A persistent problem in the related art is that the solutions require revolutionary change in reading equipment and installation of new equipment. Not only do the previously proposed solutions require very substantial investment in new technologies and equipment, but also many require obsolescence of existing data reading or processing apparatus and related systems.

PROBLEMS SOLVED BY THE INVENTION

The problems solved by this invention include, among others, the inadvertent acceptance of fraudulent data storage articles counterfeited by readily available replication methods. These data storage article include all the types of credit, debit, and identification cards mentioned above. While there have been other solutions to this problem, this invention avoids the high cost of prior solutions that require expensive cards, or entirely new card readers, and the high cost of obsoleting existing reader equipment that is still functional. This is solved by having apparatus retrofitable to existing readers. Another problem solved is the reliance on subjective human judgment required to detect and recognize visible authentication markings. The use of complex authentication criteria which are also non-visible, rather than simpler criteria using only one or two visible variables, further enhances the reliability of the present solution in detecting counterfeit data cards and the like. The problems of slow authentication and/or unreliable recognition of bar codes or other indicia are solved by the use of high frequency modulation in the present invention.

OBJECTS AND ADVANTAGES OF THE INVENTION

A general object of this invention is to provide improved security in systems using data storage articles. A particular object of this invention is a method for authenticating data storage articles for use in conjunction with existing data readers. A related object is an apparatus that can be used in conjunction with existing card readers for authenticating data storage cards. Another related object is an apparatus that can be used in conjunction with existing scanners of bar codes or of OCR-recognizable characters. Other related objects are methods and apparatus that can be used to augment the counterfeit-protection security of systems using existing card readers, scanners and information processing systems. Yet another object of this invention is to add the capability of detecting invisible codes to existing systems that scan visible indicia on data storage articles. A related object is to augment the capabilities of existing card reading, scanning, and information processing systems by allowing

reading of additional information from data storage cards. Another object is to provide improved detection capability to existing card readers, scanners and information processing systems. Related objects are methods and apparatus that can operate in conjunction with various types of existing card reading, scanning, and information processing systems, which read various types of data, and which utilize various physical principles. Other objects are authentication methods and apparatus that do not obsolete existing card reading or scanning apparatus and do not require them to be replaced. Another object is authentication apparatus that can be installed with no modification or with only minimal modification of existing card reading, scanning, or information processing equipment. Another object is authentication apparatus that can operate at high speed, to allow timely determination of authenticity while a data storage article is being read by an existing reader. Another object is authentication apparatus that utilizes existing communication capabilities of existing card reading, scanning, or information processing equipment. Other objects are authentication methods and apparatus that can prevent the completion of a transaction by existing card reading, scanning, or information processing equipment when a data storage article is not authenticated. Another object is a physically compact authentication apparatus. Another object is an apparatus that is easy to align with existing card readers, scanners, or information processing equipment. Another object is authentication apparatus that is relatively inexpensive to manufacture and to install.

SUMMARY OF THE INVENTION

Accessory apparatus for authenticating articles is used in conjunction with existing readers or scanners of articles bearing stored data, such as credit cards or identification cards. The accessory apparatus is disposed before, after, on, under, inside, or adjacent to existing reader apparatus, to have a view of the article whose data is to be read. Information in addition to the stored data is coded on the article in non-visible indicia and is detected by the accessory authenticating apparatus. This coded additional information may be related to identification data stored in the article by the article's normal storage mechanism, such as a magnetic stripe or an embedded memory chip. The additional information may be coded in various combinations of predetermined characteristics of light emitted by the article to be authenticated when the article is irradiated with non-visible light from the accessory apparatus. The code combinations are preferably complex combinations of the various radiation characteristics. Particularly useful characteristics are unique combinations of wavelengths, combinations of absolute or relative intensities, emission time delays, and spatial patterns such as bar-codes or array codes. The article is irradiated at a high enough frequency (above 10,000 Hz modulation) for rapid determination of authenticity, and for reading and decoding standard bar codes. Visible and/or audible indicators alert a banker, merchant or other user when the authentication process detects an invalid card. With certain arrangements, an invalid card may be blocked from being read by the existing reader. The accessory apparatus may be connected to interrupt the normal communication channel of the existing reader or scanner with which it is used, when an article fails to be authenticated.

Other objects, features, and advantages will become apparent from the detailed description of the preferred embodiment examples and their illustrations in the drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a functional schematic diagram of a first embodiment made in accordance with the present invention.

FIG. **2** is a functional schematic diagram of a second embodiment.

FIG. **3** is a functional schematic diagram of a first preferred embodiment.

FIG. **4** is a perspective drawing of a second preferred embodiment.

FIG. **5** is a perspective drawing showing the embodiment of FIG. **4** in relation to the existing apparatus with which it is used.

FIG. **6** is a perspective drawing of a third preferred embodiment.

FIG. **7** is a perspective drawing showing the embodiment of FIG. **6** in relation to the existing apparatus with which it is used.

FIG. **8** is a perspective drawing of a fourth preferred embodiment.

FIG. **9** is a perspective drawing showing the embodiment of FIG. **8** in relation to the existing apparatus with which it is used.

FIG. **10** is a perspective drawing of a fifth preferred embodiment.

FIG. **11** is a perspective drawing showing the embodiment of FIG. **10** in relation to the existing apparatus with which it is used.

FIG. **12** is a schematic diagram of an embodiment of an optical subsystem made in accordance with the invention.

FIG. **13** is a schematic diagram of another embodiment of an optical subsystem

FIG. **14** is a schematic diagram of an electronic subsystem used in an embodiment.

FIG. **15** is a partially cutaway perspective drawing of a detail of an alternative embodiment.

FIG. **16** is a perspective drawing of a detail of another alternative embodiment.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The authentication method of the present invention is intended to be used with existing card-reading means, such as existing "swipe readers" commonly used to read credit cards or debit cards. The data storage cards used in this method have at least two sets of indicia or codes containing data. One set consists of the indicia or codes readable by existing card-reading means. A second set consists of indicia that are invisible when irradiated with light in the visible spectrum but are detectable when irradiated with non-visible light. An add-on apparatus is used to irradiate data storage cards with non-visible light, detecting the non-visible indicia to determine the authenticity (or lack of authenticity) of the data storage card. In one variation of the method, each data storage card is exposed to the existing card-reading means to read the codes that the existing reader can read, and the resulting output of the existing reader is either allowed to pass or blocked. In another variation, the existing reader is allowed to read each data storage card only if that data storage card is authentic. This is accomplished by physically blocking entry of the card from the existing reader with a mechanical stop actuated by a failed authentication signal, by sending an enabling signal to the existing reader, or by

controlling the power input to the existing reader. In a method where the existing reader is allowed to read the card and its normal data output is allowed to pass, an authentication code can be added to that data stream. The authentication code can be as short as one binary bit appended or prefixed to the existing reader output, indicating either authentication or failure of authentication. One simple method of determining authenticity utilizes a pre-defined relationship between the codes read by the existing reader and the non-visible codes read by the add-on apparatus, giving a positive authentication result if the relationship is true for the specific data storage card being tested.

In general, the detection or reading of the non-visible codes by the add-on apparatus can occur before, after, or simultaneously with reading of the visible of magnetic codes by the existing reader. In a preferred method, the non-visible codes are detected by modulating the non-visible light at a predetermined high frequency (preferably above 10,000 Hertz), and the fluorescent light excited by the irradiation is selectively detected at the modulation frequency. All of the methods described above can be used with existing readers of many types, including magnetic stripe readers, optical character recognition (OCR) readers, bar-code scanners, magnetic character readers, CD-ROM drives, and the like.

FIG. **1** is a functional schematic diagram illustrating a first embodiment of apparatus made in accordance with the present invention. An existing reader **20** normally reads a data storage article **10**, such as a credit or identification card, typically making use of magnetic or optical coding of the data stored in data storage article **10**. Data storage article **10** bears two kinds of information: the existing stored data **110** typically coded in magnetic or visible optical form, and additional indicia **120** made for the purpose of authentication by the present invention. Indicia **120** are not visible when illuminated only by light in the visible spectrum. They may be designated "non-visible codes." The existing reader apparatus **20** has an existing decoder **40**, which typically processes signals detected by existing reader to decode the signals into digital data. Decoder **40** may be and often is an integral part of existing reader apparatus **20**, but is shown as distinct in FIG. **1** to clarify its function. In existing applications, decoder **40** would normally be connected directly to a modem **60** or to a communication terminal to communicate the decoded data to a remote location for authorization of a transaction, using a communication channel **70**, which could be a telephone connection to a remote computer, for example. For understanding the invention, it is convenient to think of the example of an existing reader **20** as a magnetic stripe reader, with a slot through which a user such as a retail merchant passes a credit card. Its decoder **40** might be integrated in the same outer housing, and it might communicate with a remote host computer through a modem **60** when a merchant dials to the remote computer.

In accordance with the present invention, an add-on probe **30** is attached to existing reader **20**, or placed adjacent to it as shown in FIG. **1**. Add-on probe **30** must have an optical view of at least a selected portion of data storage article **10** for both irradiation of that portion and detection of light from it. Add-on probe **30** acts in conjunction with the existing reader **20**, and with a base system **50**, a relay switch **80**, and an over-ride **90** to authenticate a data storage article **10** presented to the existing reader **20**. Add-on probe **30** comprises a housing, a high-frequency modulated source of non-visible light, one or more detectors of fluorescent light excited by that light source, an optical system including wavelength-selective filters, fiber-optic elements carrying both the non-visible irradiating light and the fluorescent light excited by it, and a wiring cable carrying both excitation for the light source from base system **50** and detected signals to base system **50**. Base system **50** comprises a source of excitation for the irradiating source, electronic signal processing circuitry, an indicator **55**, and at least one electrical output. Indicator **55** may be an audible indicator and/or a visible display for indicating to the user whether or not the data card or other data storage article was authenticated. Over-ride **90** allows a user to over-ride normal operation by manual intervention in unusual circumstances, such as equipment malfunction or direct authorization of a transaction. Base system **50** may be integrated with add-on probe **30** in a single housing. In any event, the housing of add-on probe **30** is adapted to fit the physical characteristics of existing reader **20** as later examples will show in more detail.

In FIG. **1**, base system **50** communicates with relay switch **80**, which gates the normal output from existing decoder **40**, which is typically a communication output. If the electronic signal processing circuitry of base system **50** produces a positive authentication signal, relay switch **80** passes the output of decoder **40** to modem **60**. If base system **50** fails to authenticate the card, relay switch **80** may block the transmission of data from decoder **40** to modem **60**, and may also send a "failed authentication" signal to modem **60** in place of (or in addition to) the existing reader's data, to be transmitted over communication channel **70** to a remote location. Simply blocking the transmission of data from the existing reader can prevent the transaction from being completed with an invalid card, but transmission of the data in addition to a failed authentication signal can inform the remote computer of the association of that data with failed authentication. That combined information can be used to prevent further authorizations for the same invalid card in future transactions.

Add-on probe **30** and base system **50** may be constructed using high frequency modulated sources, wavelength-selective filters, optical components, fluorescent-light detectors, and signal-processing electronics as described below with reference to FIGS. **3**, **12**, **13** and **14**. It will be apparent from those descriptions that various ways of partitioning the apparatus between add-on probe **30** and base system **50** are possible.

FIG. **2** is a functional schematic diagram of a second embodiment. The embodiment illustrated in FIG. **2** operates similarly to that of FIG. **1**, except that a provision is added for changing the program of base system **50** upon instructions **230** transmitted from a host computer or remote terminal through modem **240**. In an application to existing apparatus, such as an ATM machine having a local computer controller, that computer may be used to transmit instructions **230** to base system **50**.

The major functional components of the apparatus of this invention may be partitioned between an add-on probe **30** and a base system **50** in a number of ways for different applications. For most common applications, the first preferred embodiment has the partitioning shown in FIG. **3**, which illustrates what is believed to be the best mode of practicing the invention. In the partitioning shown in FIG. **3**, only a fiber-optic connection **35** is within the add-on probe **30**, carrying non-visible irradiating light to the data storage card **10** and carrying fluorescent light from non-visible codes **120** on the data storage card back to base system **50**. All other major components are in base system **50**. Base system **50** comprises an optical subsystem **130**, an electronic subsystem **140**, and its input/output port **150**. Electrical connections are made from electronic subsystem **140** to relay **80** and to indicators **55**.

FIG. 4 is a perspective drawing of a second preferred embodiment in which a housing 310 containing the functional elements of add-on probe 30 is adapted to fit against an existing reader 20 and automatically align to it. Housing 310 has a slot 320 similar to a slot in an existing magnetic or optical reader 20. Extended portions 340 of housing 310 surround two sides of a recess 330 which fits existing reader 20, and slot 320 is situated to align with slot 25 of existing reader 20, when housing 310 and existing reader 20 are adjacent. An interconnecting cable 350 connects add-on probe 30 to base system 50. FIG. 5 illustrates the embodiment of FIG. 4 in relation to the existing apparatus 20 with which it is used. (Existing apparatus 20 is shown with dashed lines.) This embodiment is used "upstream" of an existing reader: i.e. the data storage article is passed through the slot 320 before passing through slot 25. Slot 320 contains in at least one of its side walls the optical interface needed for add-on probe 30. In one arrangement of the type of apparatus shown in FIG. 4, illumination of the data storage article by non-visible light and detection of fluorescent light from invisible codes 120 is done on the surface of the article opposite the surface used for its existing magnetic or visible optical data. Fasteners of various types may be used to hold housing 310 and existing reader 20 together if needed. For example the housings could be attached with double-sided adhesive tape to a common base plate extending under both housings.

FIG. 6 is a perspective drawing of a third preferred embodiment. This embodiment is similar to that of FIG. 4, but is designed to be used "downstream" from the existing reader: the data storage article is passed through ("swiped" through) slot 320 after passing through slot 25 of existing reader 20. Interconnecting cable 350 is shown at the bottom surface of housing 410 to illustrate an alternative arrangement of the light source and detector or fiber-optical link(s). In this embodiment, interconnecting cable 350 may be a fiber-optic cable. The light source and detector or fiber-optical link(s) may be positioned to illuminate an edge of the data storage card and to detect light excited at the card edge. This arrangement is used with cards having invisible coding incorporated within a card in such a way that they are detectable at an edge of a card. Such cards might have coded fluorescent substances incorporated into all of the card substrate material or might have discrete layers incorporating invisible codes detectable at their edges. There is no causal or other relationship between the two features illustrated in FIG. 6 (downstream swipe and edge illumination/detection) that would require them to be used together in the same embodiment. FIG. 7 is a perspective drawing showing the embodiment of FIG. 6 in relation to the existing apparatus 20 with which it is used.

FIG. 8 is a perspective drawing of a fourth preferred embodiment. Housing 510 is similar to both housing 310 of FIG. 4 and housing 410 of FIG. 6, but has an aperture 530 designed to contain and hold the entire existing reader 20. Side portions 540 and end portion 550 enclose the aperture to hold the existing reader 20 in place as illustrated in FIG. 9. Slot 560 aligns with the slot 25 of existing reader 20 to provide an entrance or exit path for a data card or the like. Slot 320 also aligns with slot 25 and contains in a side wall the optical interface needed for the add-on probe 30. FIG. 9 is a perspective drawing showing the embodiment of FIG. 8 in relation to the existing apparatus with which it is used. The embodiment of FIG. 8 and FIG. 9 may be used either upstream or downstream of existing reader 20.

FIG. 10 is a perspective drawing of a fifth preferred embodiment for use with an existing optical scanner, and FIG. 11 is a perspective drawing showing the embodiment of FIG. 10 in relation to the existing optical scanner apparatus. The embodiment of FIG. 10 has a housing 930 with a window 940 and an interconnecting cable 950. Housing 930 contains an add-on probe 30, which in this embodiment incorporates a scanning function. Existing scanner 910 has a window 920 and interconnecting cable 915. Add-on probe housing 930 is attached to the existing scanner housing to align window 940 with existing scanner window 920, so that the scanner of add-on probe 30 can scan the same article being scanned by the existing scanner.

FIG. 12 is a schematic diagram of an embodiment of an optical subsystem 130 made in accordance with the invention. In the embodiment of FIG. 12, add-on probe 30 includes the entire optical subsystem 130 shown. This is a different partitioning from the preferred partitioning shown in FIG. 3 and is used here for clarity in describing the optical subsystem.

A data storage article 10 is moving through or past add-on probe 30, and carries non-visible codes 120. The optical subsystem 130 of FIG. 12 has a modulated source 1110 of non-visible light, and may optionally have a modulated source 1120 of visible and/or infrared light as well. Source 1110 may be a UV source such as a high-pressure mercury lamp, for example. In FIG. 12, the electrical excitation of non-visible light source 1110 (and optionally 1120) comes from base system 50. Non-visible light source 1110 may be self-modulating as in Hopkins U.S. Pat. No. 4,642,526. Non-visible light propagates through optical path 1115, fiber-optic interface 1145, and fiber-optic connection 35 to illuminate data storage article 10. (Fiber-optic elements may be used for other parts of optical path 1115 as well.) Fiber-optic interface 1145 may include a lens, aperture, or slit, as may the output end of fiber-optic connection 35. Fiber-optic connection 35 also carries fluorescent light excited by the non-visible light back along optical path 1115 into add-on probe 30. With suitable fiber material and construction, the same optical fiber may be used for both non-visible irradiation light and for the fluorescent light emitted by non-visible codes 120. An optical filter 1150 selects a portion of the fluorescent light to be detected by a detector 1140. The electrical output of detector 1140 is sent to base system 50 for interpretation, as described below with reference to FIG. 13.

FIG. 13 is a schematic diagram of another embodiment of an optical subsystem 130. As in FIG. 12, add-on probe 30 includes the entire optical subsystem. For the purpose of describing this subsystem, data storage article 10 is assumed to be stationary. This embodiment has a scanner 1160 for scanning a beam of non-visible light across a selected portion of data storage article 10. Scanner 1160 may be an oscillating mirror, for example, or any conventional scanner suitable for the non-visible irradiating light from source 1110. FIG. 13 also shows optional beam splitter 1130, optionally plural optical filters 1150, and optionally plural detectors 1140. Fluorescent light from non-visible codes 120 propagates along return optical path 1116. With either singular or plural detectors 1140, each detector has an output signal channel, carried to base system 50 via an interconnecting cable. As in the embodiment of FIG. 12, fiber-optic elements may be used for portions of optical path 1115 or return optical path 1116.

FIG. 14 is a schematic diagram of electronic subsystem 140 used in an embodiment of base system 50. Base system 50 has an input signal from the detector of 1140 of add-on probe 30. In versions that have multiple detectors 1140, a multiplexer 1175 multiplexes signals from the various detec-

tors channels. In versions with only a single detector, multiplexer **1175** is unnecessary. At analog-to-digital converter **1180** the detector analog signals are converted to digital signals. The digital signals are sent as inputs to memory **1190**, microcomputer **1200** and recognition logic **1170**, which interpret the digital signals to determine whether the invisible codes **120** detected correspond to authentic data storage articles. That determination is made under control of a program stored in a program memory associated with microcomputer **1200**. Memory **1190**, microcomputer **1200** and recognition logic **1170** are shown here as distinct elements, but it will be appreciated that their functions may all be performed by a microcomputer with on-board memory and particularly by a digital signal processor (DSP). The recognition logic or its equivalent microcomputer program uses conventional recognition algorithms to recognize the codes represented by invisible codes **120**. The result of determining authenticity of the data storage article is either positive (authenticated) or negative (not authenticated). The result is indicated to a user of this apparatus by indicators **55**, preferably both audible and visible indicators. At the same time, the authentication result is used to control relay **80**. In the simplest method, relay **80** is used either to allow the output of existing reader **20** to pass to modem **60** if the authentication result is possible, or to block that output if the authentication result is negative. In other methods, the authentication result may be appended or prefixed to the normal output of existing reader **20**, to inform a host system of the authentication result. Input/output port **1220** allows any input or output of microcomputer **1200**, but especially for re-programming of the instructions of microcomputer **1200**, such as in using the program change instructions **230** of FIG. **2**.

While the invention has been described in terms of particular partitioning of functions between an add-on probe **30** and a base system **50**, these partitionings were made to describe the invention more clearly. The various functions can be partitioned differently between these two major portions of the apparatus without changing the operation of the invention. One way of re-partitioning the apparatus is to keep only a fiber-optic element as add-on probe **30**, and partition all other components of the apparatus into base system **50**. Another way of re-partitioning the apparatus is to put all of the elements in a single housing acting as the add-on probe **30**, and integrating the base system **50** elements into that single housing.

FIG. **15** is a partially cutaway perspective drawing of a detail of an alternative embodiment in which add-on probe **30** has an optical fiber connection **35** to existing reader **20**. Optical fiber connection **35** passes through a hole drilled in the housing of existing reader **20**, and terminates in a suitable optical terminal at the wall of slot **25**. The termination of optical fiber connection **35** may include a lens, aperture, or slit. The terminated end of optical fiber connection **35** is disposed to illuminate a data storage card passing through slot **25** and to transmit fluorescent light from invisible codes **120** on the data storage card back to an optical filter **1150** and a detector **1140** in add-on probe **30**.

FIG. **16** is a perspective drawing of a detail of another alternative embodiment, in which optical fiber connection **35** is disposed adjacent to either the entrance end or exit end of slot **25** in existing reader **20**.

When any of these embodiments are used, add-on probe **30** is placed adjacent to existing conventional reader **20** or attached to it. Most of the versions of add-on probe **30** align automatically with the slot or with the scan field of existing reader **20** (or **910**). Otherwise add-on probe **30** is aligned to allow the same data storage article, such as a data card, to be read by both the existing reader and add-on probe **30**. The normal output of existing reader **20** is routed through relay **80** as illustrated in FIGS. **1** or **2**. Operation of base system **50** is automatic, and may be programmed to either block the output of existing reader **20** when a data storage article is not authenticated, or to augment reader **20** output with an authentication code. An alternative method of using the invention is to allow a host system to make the determination of authenticity on the basis of information transmitted by base system **50**. This may be done, for example, by comparing detected invisible codes **120** with predetermined codes, or with information codes received in the same transmission from existing reader **20**, or by using some combination of these codes.

Other embodiments of the invention will be apparent to those skilled in the art from a consideration of this specification or from practice of the invention disclosed herein. For example, the data storage articles to which the invention may be applied need not be cards, but can be any type of articles bearing data, such as computer magnetic storage disks, CD-ROM disks, magnetic digital data tapes, video tapes, video disks, game cartridges, analog or digital audio tapes, bank checks, event admission tickets, transportation tickets, passes, food stamps, and coupons. In each case the apparatus and methods of this invention may be adapted as an adjunct to the existing equipment without extensive modification of the existing equipment or at least without obsoleting the existing equipment. It is intended that the specification and examples be considered as exemplary only, with the true scope and spirit of the invention being defined by the following claims.

Having described our invention, we claim:

1. A method for authenticating data storage cards for use in conjunction with existing card-reading means, comprising the steps of:

a) providing data storage cards bearing at least two sets of indicia including

first indicia that are invisible when irradiated with light in the visible spectrum but are detectable when irradiated with non-visible light and

second indicia readable by said existing card-reading means,

b) irradiating said data storage cards with said non-visible light,

c) detecting said first indicia to determine the authenticity or lack thereof for each of said data storage cards, and

d) optionally exposing each of said data storage cards to said existing card-reading means to read said second indicia.

2. A method as in claim **1** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said exposing step (d) is performed only if each said data storage card is authentic.

3. A method as in claim **1** for authenticating data storage cards for use in conjunction with existing card-reading means, further comprising the step of:

e) indicating authenticity or lack thereof for each of said data storage cards according to the result of said detecting step (c).

4. A method as in claim **1** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said irradiating step (b) further comprises the step of modulating said non-visible light at a predetermined frequency, and

said detecting step (c) further comprises the step of selectively detecting fluorescent light at said predetermined frequency.

5. A method as in claim 4 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said predetermined frequency is equal to or greater than 10,000 Hertz.

6. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said detecting step (c) further comprises the step of comparing said first and second indicia according to predetermined criteria.

7. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said exposing step (d) is performed before said irradiating and detecting steps (b) and (c).

8. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said exposing step (d) is performed after said irradiating and detecting steps (b) and (c).

9. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said exposing step (d) is performed simultaneously with said irradiating and detecting steps (b) and (c).

10. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said providing step (a) includes providing at least said second indicia in magnetic patterns, and

said exposing step (d) is performed by using existing card-reading means capable of reading magnetic patterns and by reading said second indicia magnetically.

11. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said providing step (a) includes providing at least said second indicia in a magnetic stripe, and

said exposing step (d) is performed by using existing card-reading means capable of reading a magnetic stripe and by reading said second indicia magnetically.

12. A method as in claim 11 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said existing card-reading means has a slot, and wherein said exposing step (d) is performed using existing card-reading means by moving said magnetic stripe through said slot of said existing card-reading means.

13. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said providing step (a) includes providing at least said second indicia as an optical bar code, and

said exposing step (d) is performed by using existing card-reading means capable of reading an optical bar code and by reading said second indicia optically.

14. A method as in claim 13 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said exposing step (d) is performed using existing card-reading means to scan said optical bar code.

15. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said providing step (a) includes providing at least said second indicia as optical characters, and

said exposing step (d) is performed by using existing card-reading means capable of reading and recognizing optical characters, by reading said second indicia optically, and by recognizing said optical characters.

16. A method as in claim 1 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said existing card-reading means has an existing output, further comprising the steps of

(f) enabling said existing output if each of said data storage cards is authentic, and

(g) blocking said existing output if each of said data storage cards is not authentic, respectively.

17. A method as in claim 8 for authenticating data storage cards for use in conjunction with existing card-reading means, further comprising the steps of

(h) allowing said exposing step (d) for each of said data storage cards if it is authentic, and

(i) preventing said exposing step (d) for each of said data storage cards if it is not authentic, respectively.

18. A method as in claim 17 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said allowing step (h) is performed by allowing each of said data storage cards to enter said existing card-reading means if it is authentic, and

said preventing step (i) is performed by preventing each of said data storage cards from entering said existing card-reading means if it is not authentic, respectively.

19. A method as in claim 17 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said allowing step (h) is performed by providing a first electrical input to enable said existing card-reading means, and

said preventing step (i) is performed by providing a second electrical input to disable said existing card-reading means, respectively.

20. A method as in claim 17 for authenticating data storage cards for use in conjunction with existing card-reading means, wherein

said allowing step (h) is performed by providing electrical power to said existing card-reading means, thereby enabling operation of said existing card-reading means, and

said preventing step (i) is performed by withholding electrical power from said existing card-reading means, thereby disabling operation of said existing card-reading means, respectively.

21. An apparatus for authenticating data storage cards for use in conjunction with existing card-reading means, comprising:

a) a housing having first and second ends and a card slot communicating between said first and second ends, said card slot being adapted for alignment with said existing card-reading means,

b) a source of irradiating light characterized by having a peak wavelength outside the visible spectrum, said source being adapted for irradiating said data storage cards while they are within said card slot,

c) one or more detectors of light emitted by said data storage cards in response to said irradiating light, each of said detectors producing a first electrical signal depending on one or more characteristics of said emitted light,

d) signal processing means responsive to at least one of said first electrical signals to produce a second electrical signal indicative of the authenticity of said data storage cards, and

e) output means responsive to said second electrical signal to indicate authenticity status of said data storage cards.

22. An apparatus as in claim **21** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said output means comprises a visible indicator recognizable by a human user of the apparatus.

23. An apparatus as in claim **21** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said output means comprises an audible signal recognizable by a human user of the apparatus.

24. An apparatus as in claim **21** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said output means comprises an electrical output recognizable by said existing card-reading means.

25. An apparatus as in claim **24** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said electrical output comprises an electrical power input for energizing said existing card-reading means.

26. An apparatus as in claim **21** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said existing card-reading means has an existing slot, and said card slot is aligned with said existing slot in said existing card-reading means.

27. An apparatus as in claim **21** for authenticating data storage cards for use in conjuncnon with existing card-reading means, wherein said first end of said housing is disposed so that said data storage cards may pass through said card slot before entering said existing card-reading means.

28. An apparatus as in claim **21** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said first end of said housing is disposed so that said data storage cards may pass through said card slot after exiting said existing card-reading means.

29. An apparatus for authenticating data storage articles for use in conjunction with existing article-scanning means, comprising:

a) a housing having a window and means for attaching said housing to said existing article-scanning means, said housing being adapted for alignment with said existing article-scanning means,

b) a source of irradiating light characterized by having a peak wavelength outside the visible spectrum, adapted for irradiating said data storage articles through said window in said housing,

c) one or more detectors of light emitted through said window by said data storage articles in response to said irradiating light, each of said detectors producing a first electrical signal depending on one or more characteristics of said emitted light,

d) signal processing means responsive to at least one of said first electrical signals to produce a second electrical signal indicative of the authenticity of said data storage articles, and

e) output means responsive to said second electrical signal to indicate authenticity status of said data storage articles.

30. An apparatus for authenticating data storage cards for use in conjunction with existing card-reading means, comprising:

a) a first light guide characterized by being transmissive to non-visible light, said first light guide being adapted for irradiating said data storage cards with said non-visible light while said existing card-reading means are in use,

b) a second light guide characterized by being transmissive to fluorescent light emitted by said data storage cards in response to said non-visible light, said second light guide being adapted for transmitting said fluorescent light while said existing card-reading means are in use,

c) a source of said non-visible light characterized by having a peak wavelength outside the visible spectrum, said source being adapted for irradiating said data storage cards through said first light guide,

d) one or more detectors adapted for detecting said fluorescent light emitted through said second light guide by said data storage cards in response to said irradiating light, each of said detectors producing a first electrical signal depending on one or more characteristics of said emitted fluorescent light,

e) signal processing means responsive to at least one of said first electrical signals to produce a second electrical signal indicative of the authenticity of said data storage cards, and

f) output means responsive to said second electrical signal to indicate authenticity status of said data storage cards.

31. An apparatus as in claim **30** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said first light guide (a) and said second light guide (b) are combined in a single light guide characterized by being transmissive to both said non-visible light and said fluorescent light.

32. An apparatus as in claim **30** for authenticating data storage cards for use in conjunction with existing card-reading means, wherein said first light guide (a) and said second light guide (b) are combined in a single fiber-optic cable characterized by having fibers transmissive to both said non-visible light and said fluorescent light.

33. An apparatus as in claim **21**, wherein said source of irradiating light is selected from the list consisting of a high-pressure mercury vapor lamp, a non-visible laser, a non-visible light-emitting diode, and a non-visible arc lamp.

34. An apparatus as in claim **29**, wherein said source of irradiating light is selected from the list consisting of a high-pressure mercury vapor lamp, a non-visible laser, a non-visible light-emitting diode, and a non-visible arc lamp.

35. An apparatus as in claim **30**, wherein said source of irradiating light is selected from the list consisting of a high-pressure mercury vapor lamp, a non-visible laser, a non-visible light-emitting diode, and a non-visible arc lamp.

36. An apparatus as in claim **21**, wherein said signal processing means comprise:

a) an analog-to-digital converter for converting said first electrical signal to digital form,

b) a memory for storing at least said digital form of said first electrical signal,

c) recognition logic for recognizing said digital form of said first electrical signal, and

d) a microcomputer for generating said second electrical signal indicative of the authenticity of said data storage cards.

37. An apparatus as in claim **29**, wherein said signal processing means comprise:

a) an analog-to-digital converter for converting said first electrical signal to digital form,

b) a memory for storing at least said digital form of said first electrical signal,

c) recognition logic for recognizing said digital form of said first electrical signal, and

d) a microcomputer for generating said second electrical signal indicative of the authenticity of said data storage articles.

38. An apparatus as in claim **30**, wherein said signal processing means comprise:

a) an analog-to-digital converter for converting said first electrical signal to digital form,

b) a memory for storing at least said digital form of said first electrical signal,

c) recognition logic for recognizing said digital form of said first electrical signal, and

d) a microcomputer for generating said second electrical signal indicative of the authenticity of said data storage cards.

39. An apparatus as in claim **21**, wherein said signal processing means comprise a digital signal processor.

40. An apparatus as in claim **29**, wherein said signal processing means comprise a digital signal processor.

41. An apparatus as in claim **30**, wherein said signal processing means comprise a digital signal processor.

42. An apparatus as in claim **30**, wherein said first and second light guides are inserted through holes in said existing card-reading means.

43. An apparatus as in claim **31**, wherein said single light guide is inserted through a hole in said existing card-reading means.

44. An apparatus as in claim **32**, wherein said fiber-optic cable is inserted through a hole in said existing card-reading means.

45. An apparatus as in claim **21**, wherein said existing card-reading means are selected from a list of reading means consisting of magnetic stripe readers, magnetic tape readers, magnetic character readers, optical character readers, IC card readers, memory card readers, game cartridge readers, bar-code scanners, CCD scanners, CD-ROM readers, and RF tag readers.

46. An apparatus for authenticating data storage articles for use in conjunction with existing article-reading means, comprising:

a) a housing, said housing being adapted to be aligned with said existing article-reading means;

b) a source of irradiating light characterized by having a peak wavelength outside the visible spectrum, said source being adapted to irradiate said data storage articles;

c) one or more detectors of light emitted by said data storage articles in response to said irradiating light, each of said detectors producing a first electrical signal depending on one or more characteristics of said emitted light;

d) signal processing means responsive to at least one of said first electrical signals to produce a second electrical signal indicative of the authenticity of said data storage articles; and

e) output means responsive to said second electrical signal to indicate authenticity status of said data storage articles.

* * * * *

United States Patent [19]

Gaucher

[11] **Patent Number: 4,851,651**

[45] **Date of Patent: Jul. 25, 1989**

[54] **AUTOMATIC PROGRAMMER AND DISPENSER OF MICROCIRCUIT CARDS**

[75] Inventor: **Michel M. Gaucher**, Le Mesnil Saint Denis, France

[73] Assignee: **Electronique Serge Dassault**, Saint Cloud, France

[21] Appl. No.: **30,732**

[22] Filed: **Mar. 25, 1987**

[30] **Foreign Application Priority Data**

Mar. 25, 1986 [FR] France 86 04292

[51] **Int. Cl.**[4] **G06F 15/30**

[52] **U.S. Cl.** **235/380**; 235/475

[58] **Field of Search** 235/379, 380, 475, 479, 235/492, 487; 221/121, 231, 129, 92, 175, 176; 194/210, 211; 222/2

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,317,028	2/1982	Simjiam	235/375
4,467,209	8/1984	Maurer	235/487
4,600,828	7/1986	Nogami	235/379
4,641,239	2/1987	Takesako	235/380

FOREIGN PATENT DOCUMENTS

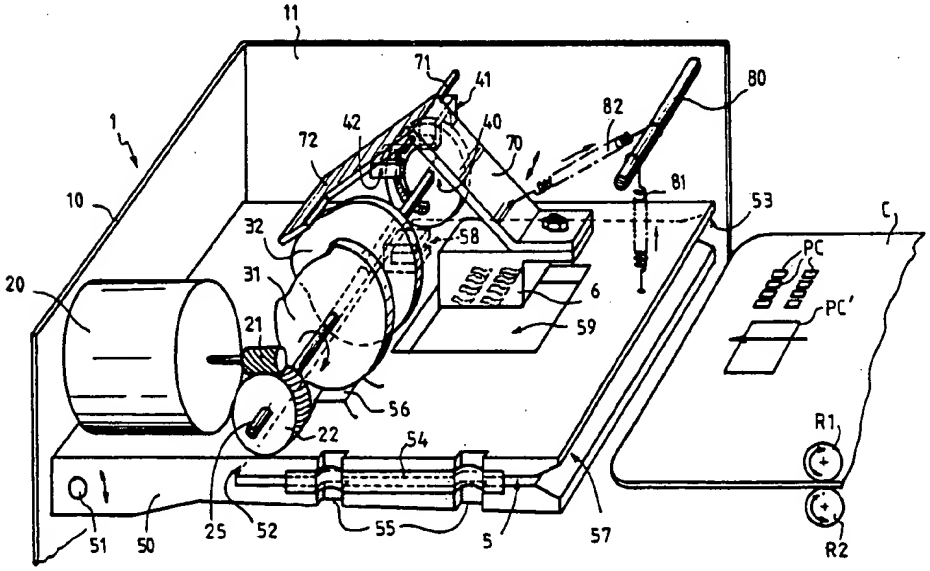
2551918	5/1977	Fed. Rep. of Germany .
3432557A1	3/1986	Fed. Rep. of Germany .
1540050	9/1968	France .
8215538	11/1984	France .
1277844	6/1972	United Kingdom .

Primary Examiner—A. D. Pellinen
Assistant Examiner—Leon K. Fuller
Attorney, Agent, or Firm—Christie, Parker & Hale

[57] **ABSTRACT**

A disk (**110**) carries containers (such as **120**) each containing a stack of cards capable of being extracted one-by-one via an orifice (**126**) when a wheel (**151**) is moved to an extraction position (**151A**). A first conveyor (**140A**) then conveys the extracted card to a programming unit (**1**) which is capable of being moved to a position enabling a card to be inserted therein without friction, and thereafter lowers a connector (**6**) onto the card. After the card has been validated and inspected, it is conveyed to a user along the first conveyor (**140A**) and then along a second conveyor (**140B**) terminating at a delivery slot (**105**). An invalid card may be directly rejected into a reject box (**180**) placed beneath the programming unit (**1**).

18 Claims, 6 Drawing Sheets



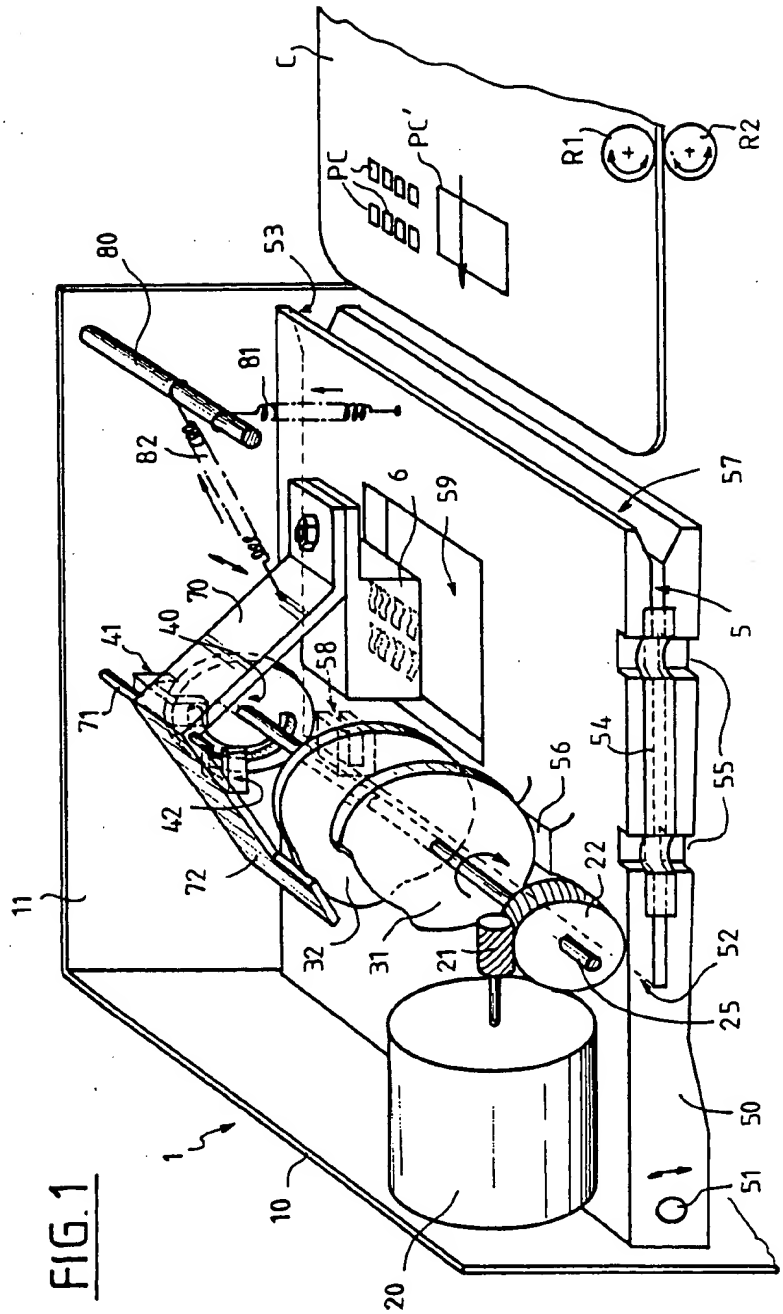

C
PC
PC'
R1
R2
80
53
81
82
6
59
57
5
70
40
41
58
71
54
56
55
42
72
22
11
32
31
21
52
25
50
1
10
Q
51
20

FIG. 1

FIG. 2

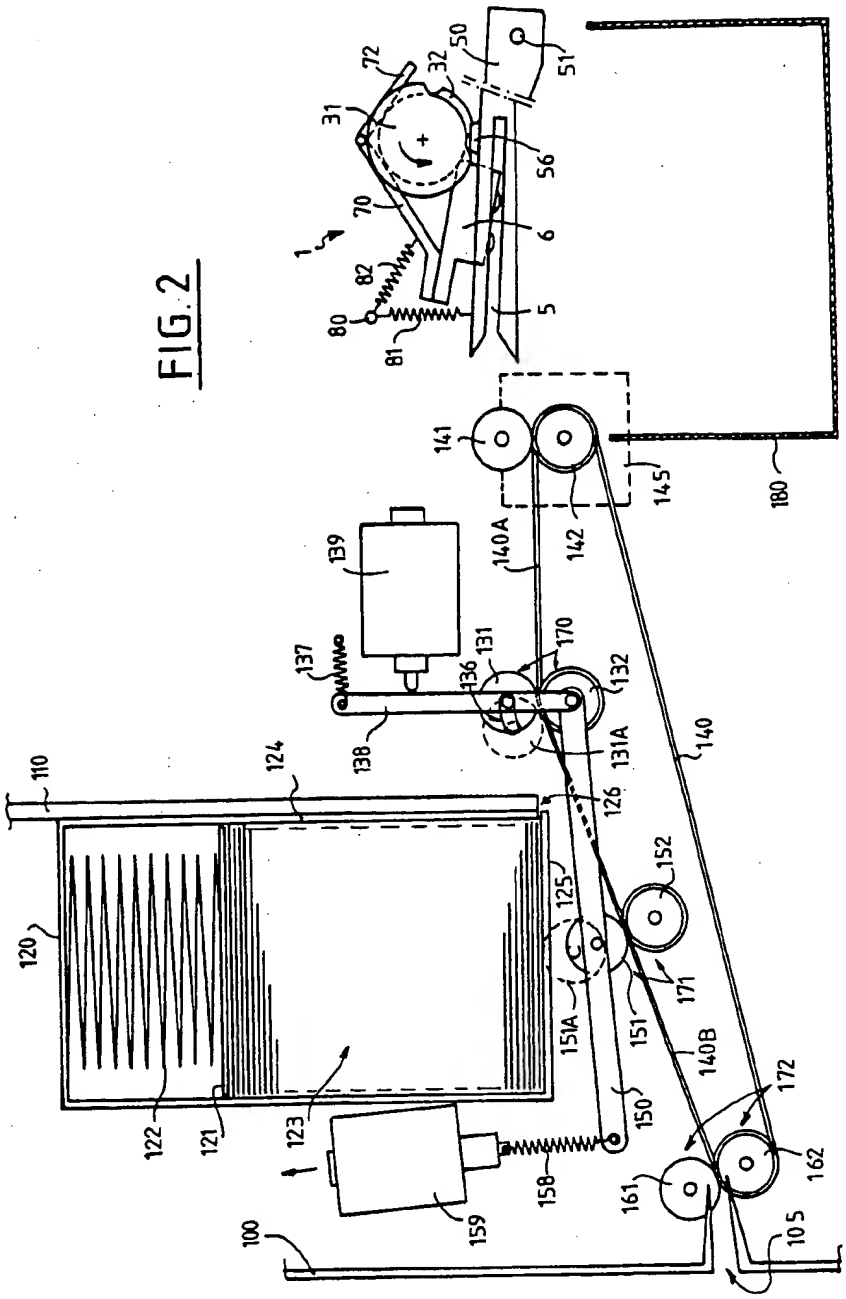

72
32
50
51
31
56
70
6
1
82
5
80
81
141
145
180
139
140A
142
137
131
170
136
132
138
131A
140
110
124
126
120
125
152
171
151
151A
140B
172
122
121
123
150
158
161
162
159
105
100

FIG. 2A

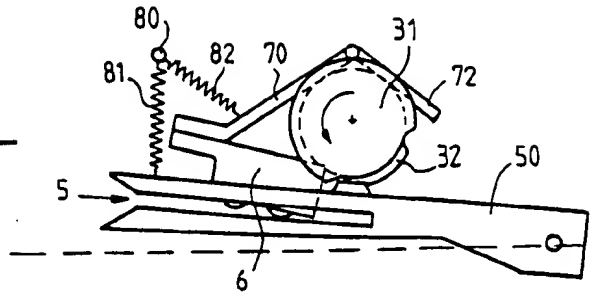


FIG. 2B

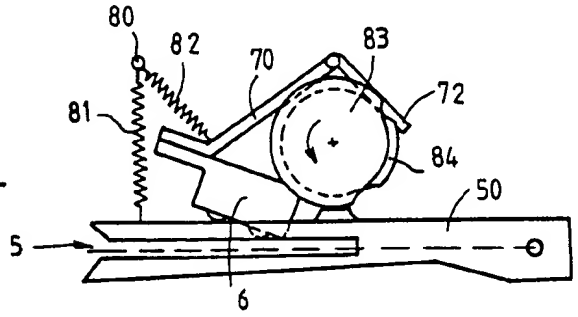


FIG. 2C

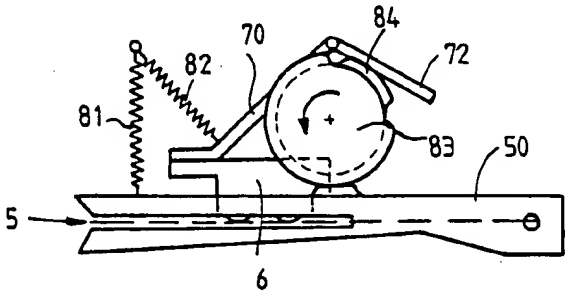


FIG. 3

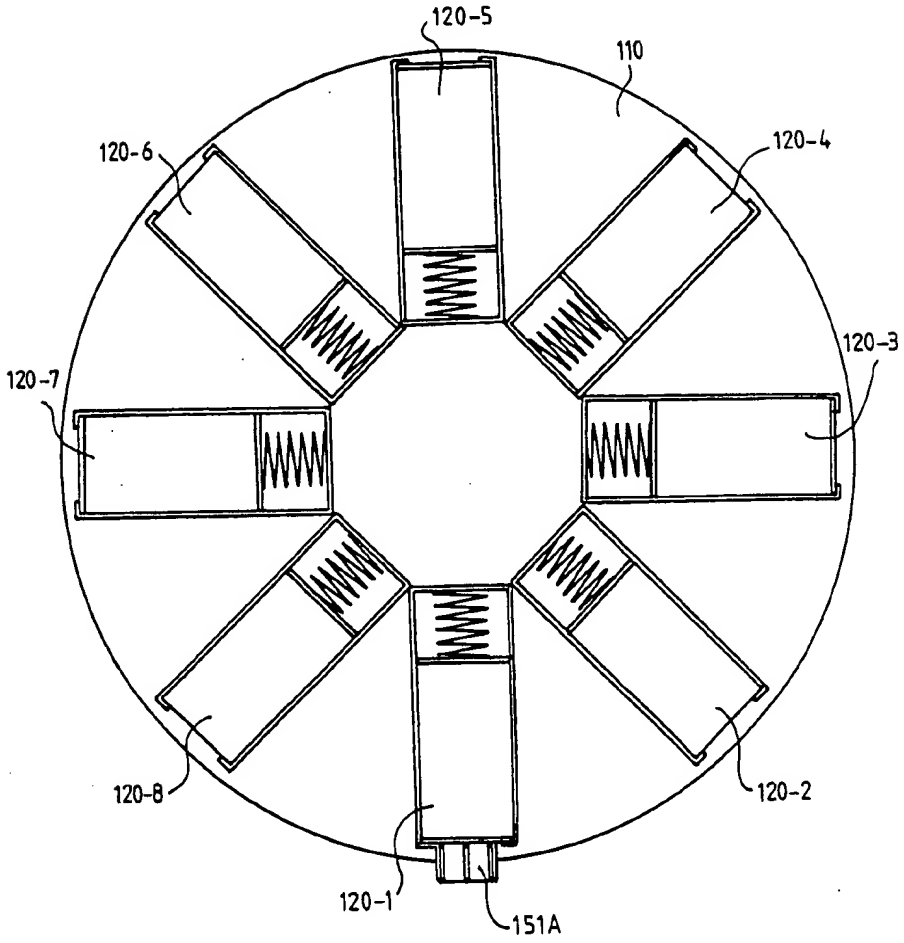


FIG. 4

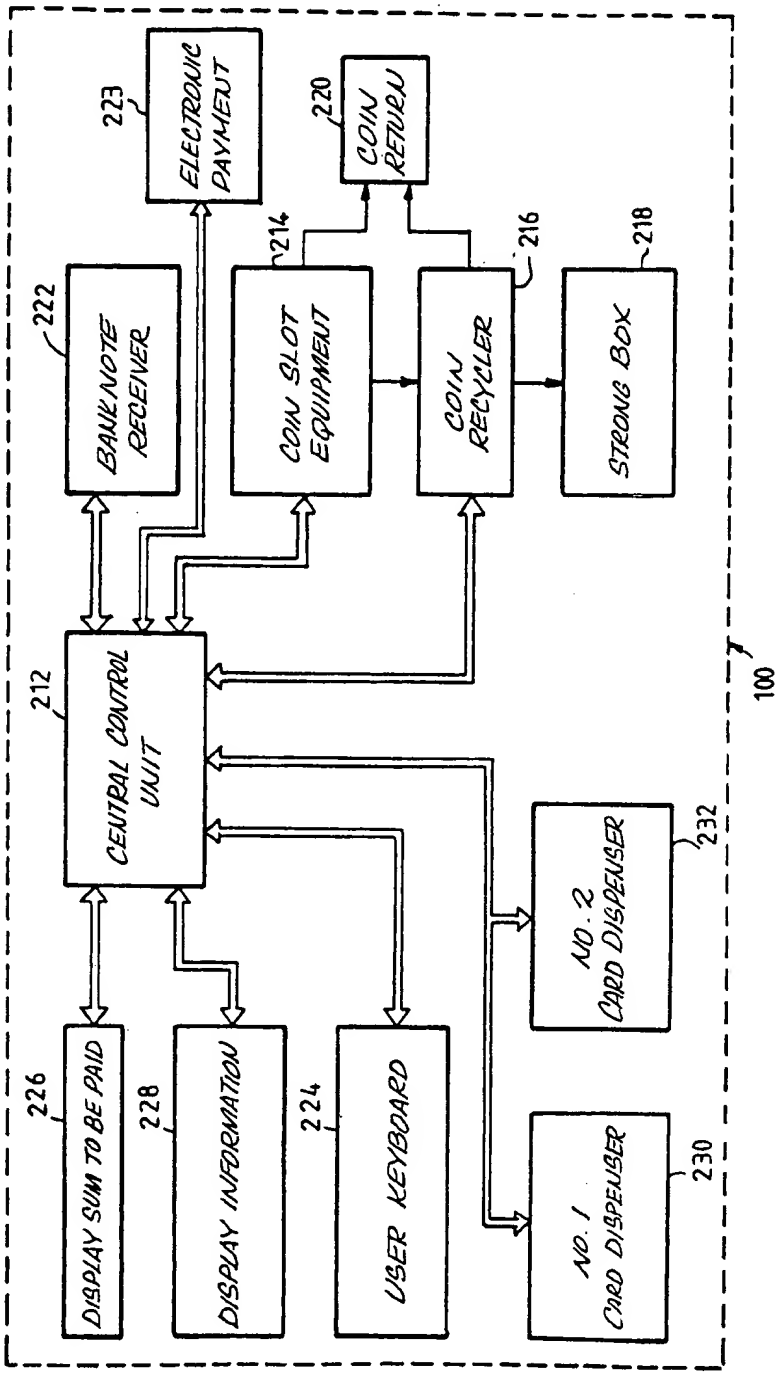

100
212
CENTRAL CONTROL UNIT
222
BANK NOTE RECEIVER
223
ELECTRONIC PAYMENT
214
COIN SLOT EQUIPMENT
220
COIN RETURN
216
COIN RECYCLER
218
STRONG BOX
226
DISPLAY SUM TO BE PAID
228
DISPLAY INFORMATION
224
USER KEYBOARD
230
NO. 1 CARD DISPENSER
232
NO. 2 CARD DISPENSER

FIG. 5

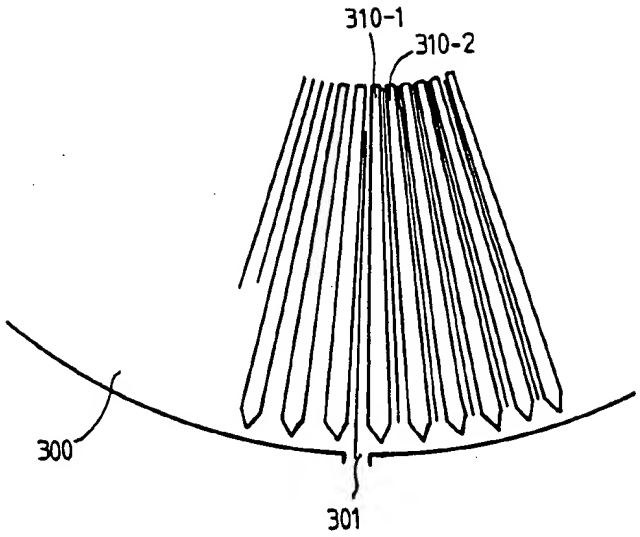
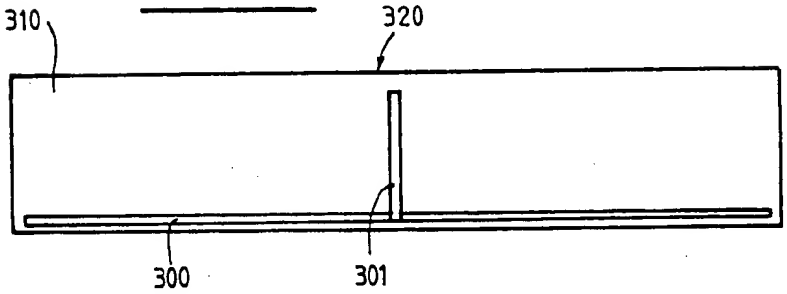


FIG. 5A



AUTOMATIC PROGRAMMER AND DISPENSER OF MICROCIRCUIT CARDS

The invention relates to dispensing microcircuit cards which are about to come into common use.

BACKGROUND OF THE INVENTION

Microcircuit cards, also known as "smart" cards, are now on sale for use with public pay phones, and such cards may have a value of 40 or 120 telephone charge units, for example. The advantage is clear: since card-accepting public phones do not contain any money they will not be broken into.

Drawbacks lie in amoritizing the cost of setting up such a smart card system and in meeting the on-going cost of dispensing suitable smart cards. These cards can be obtained not only from official telephone services, but also from numerous other retail outlets which must be paid for providing this service.

French patent application No. 86 00511 filed Jan. 15, 1986 in the name of the present applicant, describes an automatic dispenser for smart cards, which dispenser is suitable for dispensing telephone cards. Such machines reduce the cost of dispensing cards. However, they bring back the problem of machines being broken into: since smart card dispensing machines contain money, they will be worth robbing. This danger can be reduced by placing such dispensing machines in crowded locations or in locations which are under constant surveillance. However this solution is not capable of general application.

The present applicant seeks to improve the safety of smart card dispensing machines.

Thus, one aim of the invention is to provide an automatic smart card dispensing machine in which the stock of undispensed cards has no monetary value.

Another aim of the invention is to enable a smart card whose credit has been exhausted to be re-validated (i.e. reprogrammed).

SUMMARY OF THE INVENTION

The present invention provides an automatic dispenser for microcircuit cards, said dispenser comprising:

a cabinet;

dispenser control means also capable of dialog with a user, in order to verify the user's right to a card;

at least one magazine for non-valid microcircuit cards;

pick-up means suitable for extracting one card at a time from said magazine;

a first conveyor for conveying said card to a programming unit capable of validating said card; and

a second conveyor suitable for conveying a validated card to a card-dispensing slot through the wall of the cabinet.

In practice, the programming unit is also capable of verifying card validation, and the dispenser includes rejection means enabling any incorrectly validated card to be retained inside the cabinet.

Preferably, the first and second conveyors possess a common portion suitable for transferring the card into the programming unit and out therefrom.

According to another aspect of the invention, the moving programming unit has a second position in which it no longer co-operates with the first conveyor or with the common portion. Invalid cards can then be rejected directly from the conveyor into a receptacle for the purpose.

In a particular embodiment of the invention, the pick-up means comprise a roll or wheel carried on a moving lever and suitable on control for co-operating with the magazine in order to extract a card therefrom and direct it towards the first conveyor.

Advantageously, the first conveyor includes at least two pairs of wheels constituting said common portion with at least one of said wheels being motor-driven. A closed-loop belt can then pass between the wheels of each pair. The second conveyor includes at least two other pairs of wheels specific thereto, with the last such pair being placed close to the outlet slot. The belt also passes through these other pairs of wheels.

It is advantageous for one of the wheels in the intermediate pair of wheels belonging to the second conveyor to act also as a pick-up wheel.

According to yet another aspect of the invention, the card outlet from the magazine, the path along the first conveyor, and the card inlet/outlet of the programming unit are substantially in alignment.

As a result, the path defined by the two pairs of wheels belonging to the second conveyor is, in theory, at an angle relative to the path through the first conveyor. In accordance with the invention, one of the wheels situated level with the transistion is mounted as a moving wheel so as to enable the card to be tilted without losing drive continuity.

In one embodiment, the card magazine includes at least one container storing a stack of cards which are resiliently urged towards a pick-up and outlet position.

A plurality of containers of this type may be mounted on a carrousel.

In a variant embodiment, the magazine comprises a carrousel in the form of a rack suitable for storing one card in each slot of the rack, said carrousel rack being rotatably mounted inside a disk-shaped container which is closed except for a card-delivery slot located level with one of the rack slots. Said container also houses means for rotating the carrousel.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention are described by way of example with reference to the accompanying drawings, in which:

FIG. 1 is a diagrammatic perspective view of a programming unit usable in a device in accordance with the invention;

FIG. 2 is a diagrammatic side view of a first embodiment of a device in accordance with the invention;

FIGS. 2A to 2C are diagrams showing the operation of the programming unit within the FIG. 2 device;

FIG. 3 is a plan view showing a first embodiment of a carrousel constituting a card magazine in accordance with the invention;

FIG. 4 is a block diagram showing the general structure of a device in accordance with the invention from the electronic and operational points of view; and

FIGS. 5 and 5A are diagrams showing a variant embodiment of a magazine in accordance with the invention.

The accompanying drawings are, at least in part, definitive in character. They also show geometrical shapes which are difficult to describe fully. Consequently the accompanying drawings may be used not only to clarify the description, but also to contribute to the definition of the invention, where appropriate.

MORE DETAILED DESCRIPTION

The description begins with the programming unit, with reference to FIG. 1. This programming unit is the subject of French patent application No. 86 01 794, filed Feb. 18, 1986. The descriptive content of said patent application is incorporated by reference, where necessary, into the present description.

Briefly, the FIG. 1 programming unit comprises a chassis 1 having an end wall 10 and a side wall 11 which are visible in the figure. A DC motor 20 drives an endless screw 21 which cooperates with a gearwheel 22 in order to rotate a shaft 25 clockwise (as seen in FIG. 1) with the shaft 25 carrying two cams 31 and 32 together with a wheel 40 constituting a two-position angular encoder wheel.

A receptacle 5 for receiving microcircuit or "smart" cards is defined by a slot provided in a plate 50 which is pivotally-mounted about a shaft 51.

The cam 31 engages an upwardly-projecting bump 56 on the plate 50. Contact is ensured by a resilient return force provided by a spring 81 mounted between the top of the plate 50 and a rod 80.

The slot for receiving a card such as the card C has a reference edge 53 and an opposite edge including a resilient blade 54 for urging the card C towards the reference edge 53. A detector 58 vertifies that the card is properly positioned in the slot 5.

There is an opening 59 through the top wall of the plate 50 suitable for passing a connector block 6. The connector block is mounted at the end of one of the arms 70 of a bell crank hinged on a shaft 71 and having its other arm disposed to follow the cam 32 by virtue of a resilient force applied on the arm 70 by a spring 82 connected to the rod 80.

Reference is made below to this programming unit 1, or more precisely to a mirror image thereof reflected about a median vertical plane passing therethrough.

In FIG. 2, a dispenser in accordance with the inventio comprises a cabinet having a reinforced outer wall of which a portion 100 is visible, and having a slot 105 for dispensing a card to a user.

A vertical disk 110 supports a series of card containers 120. Each container 120 contains internally-mounted resilient means 122 which press against a piston 121 which in turn urges a stack of cards 123 in a downwards direction. The bottom card presses against the bottom wall 125 of the container and is capable of leaving the container via an orifice 126. There is a hole through the bottom wall 125, and a wheel 151 passes through the hole and engages the bottom card when the wheel 151 is raised to a position 151A. The wheel is raised by means of an electromagnet 159 whose rod 158 includes resilient means and is used to displace a lever 150 carrying the wheel 151.

Drive means (not shown) rotate the wheel 151 clockwise (as shown in FIG. 2) when it is in its position 151A (e.g. the belt between 132 and 151).

A card is thus extracted from the container 120, and unstacking techniques are capable of ensuring that only one card is removed at a time, e.g. by using a suitable chute.

The card then leaves along the axis of two pairs of wheels 131 and 132 and 141 and 142. These two pairs of wheels constitute a first conveyor (path 140A), for transporting the card to the programming unit 1, and for removing it from the programming unit.

A second conveyor is formed by the abovementioned two pairs of wheels, together with a third pair of wheels 161 & 162 situated close to the delivery slot 105, and co-operates therewith for card delivery. A fourth, intermediate pair of wheels is defined by the above-mentioned wheel 151 when in its rest position and a wheel 152. A belt 140 runs round a closed loop over the wheels 162, 152, 132, and 142. In other words, this belt passes between the two wheels of each pair. The motor-driven wheel 142 and the belt 140 provide the drive required for both conveyors.

A card edge detector 170, e.g. a photoelectric barrier, is placed immediately to the right of the wheels 131 and 132 (as shown in FIG. 2) i.e. downstream therefrom for cards going towards the programming unit 1. Two other photoelectric barriers 171 and 172 are placed respectively immediately to the left of the pair of wheels 151 and 152 and to the left of the pair of wheels 161 and 162, (i.e. to the downstream sides thereof for a card moving along the second conveyor from the programming unit to the delivery slot 105).

Further, the wheel 131 is specially mounted. It is mounted near the bottom of a rod 158 having resilient means 137 tendin to urge it into a vertical position. The rod 158 may be driven by the armature of an electromagnet 139 in order to tilt it leftwardly (as seen in FIG. 2) so that the wheel 131 follows a path following an arc of a circle 136, along which it is guided by its shaft. This brings the wheel 131 into a position 131A in which the tangent between the wheel in position 131A and the wheel 132 is aligned with the tangents common to pairs of wheels 151 and 152 and 161 and 162.

A box 180 is mounted beneath the programming unit 1 and extends up to its shaft 51. The other way, the box extends practically up to a point vertically below the wheels 141 & 142.

In FIG. 2, the programming unit 1 is shown in its rest position in which it is not co-operating with the pair of wheels 141 and 142 (which wheels correspond to the wheels R1 and R2 shown in FIG. 1).

This rest position is repeated in FIG. 2A. As described in the above-mentioned French patent application No. 86 01794, the programming unit 1 may, on command, begin by taking up a position 2B in which it is capable of receiving a card with substantially no friction, and then a position 2C in which the multiple connector 6 is brought into contact with the contact tabs PC on the microcircuit card.

The general operation of the device is thus as follows:

As already mentioned, a card is initally extracted from the container 120. It enters the first conveyor and the unit 1 is placed in the position shown in FIG. 2B in order to receive the card.

The programming unit 1 then passes to the connection situation shown in FIG. 2C. The card is validated or programmed, and then preferably verified prior to the unit 1 returning to the FIG. 2B position for the card to be removed therefrom. The programming unit then returns to its rest position as shown in FIG. 2A.

If verification shows that the card has been wrongly validated, for any reason whatsoever, the first conveyor is restarted in a generally rightwards direction causing the card to fall directly into the box 180. Where appropriate, the above operations are repeated using a new card taken from the magazine 120.

If the card is properly validated, it advances a little into the first conveyor. In response to an edge of the card (e.g. its leading edge) being detected by the sensors

170, and electromagnet 139 is acutated to tilt the wheel 131 into its position 131A. The card then follows the direction of the second conveyor in portion 140B of the belt. Naturally, the electromagnet 159 is released meanwhile in order to return the wheel carried by the arm 150 to its position 151. It may be noted in passing that the lever 150 is advantageously hinged coaxially with the wheel 132.

The card can then move down along belt portion 140B until it projects out through the slot 105, enabling a user to take it out from the machine. The condition of a card being presented to a user is detected by the photoelectric barrier 171. The photoelectric barrier 172 detects that the card has indeed been taken by the user within a predetermined period of time. The user is preferably reminded by an audible signal (or by other means) if the card is forgotten.

If the card is still not taken, the entire second conveyor (paths 140B and 140A) is actuated in the opposite direction and the card is held in the box 180.

A dispenser in accordance with the invention improves security in several respects: firstly relative to the card magazine itself, and secondly relative to card programming.

A first embodiment of the card magazine is shown in FIG. 3. Eight containers 120-1 to 120-8 (for example) are located on a disk 110. The container 120-1 is engaged with the wheel 151 when in its position 151A.

When the cards are manufacutred they are initially stored in the containers 120. In isolation, a container 120 is closed and cards cannot be extracted therefrom. A locking lever is unlocked solely when the container is placed on a disk such as disk 110 which has a suitable indexing and/or mechanical coding system (3 microswitches or 3 optoelectronic sensors suitably disposed) so that cards can subsequently be extracted one at a time. When containers are not in place on a disk such as the disk 110 within a dispenser in accordance with the invention, cards cannot be extracted therefrom without breaking the container.

Within the dispense, it is impossible to have a more than one card moving at the same time, since the member 151 which extracts the cards moves to its extraction position 151A under the control of a central unit, as described below, only once during each operating cycle of the machine.

Naturally, proper positioning of the container 120-1 opposite the pick-up wheel 151 is ensured by a coding wheel or an equivalent mechanical index system provided on the disk 110. Attention is now directed to card programming.

Depending on the application and the type of card concerned, card validation may consist in fully programming an entirely blank card. At the other extreme, validation may be applied to cards which are almost completely validated except for a single validation bit at a predetermined location. Naturally, numerous intermediate solutions are also possible.

For example, when the application is a telephone card, 40-unit and 120-unit cards may be placed in different ones of the containers 120-1 and 120-2 on the carrousel 110 shown in FIG. 3. These cards may be prerecorded with inscriptions defining their value in terms of telephone charge units.

Otherwise, if the cards are completely blank, means may be provided within the portion 140B of the second conveyor for visibly marking such cards so as to indicate the number of telephone charge units they are worth. If the possible range of numbers if small, such marking can be performed by rubber stamps controlled by electromagnets. If a wider range of markings is required, a printing technique may be used such as one of those described in the following French patent applications: No. 83 11444 published under the No. 2,548,804, No. 84 10380 published under the No. 2,566,705, or No. 85 01661, which has not yet been published.

A dispenser in accordance with the invention has another important advantage: regardless of the way in which a microcircuit card is programmed or validated, it is possible to provide for a card whose credit has been exhausted to be re-inserted by a user and re-validated or re-programmed by the machine after the user has paid the appropriate sum.

The user presents the card at slot 105 and the card is inserted into the machine so that it reaches its position in the first conveyor 140A (after the wheel 141 has been tilted in the opposite direction).

The user's right to the card is then verified and the card is re-validated or re-programmed. If the re-validation does not work or is impossible (with the number of occasions on which a card can be validated being preprogrammed into the card on manufacture), a new card is programmed and dispensed to the user.

Reference is made above to the user's "right" to the card. In practice this right is obtained by paying a sum of money in coin or bank notes or by any appropriate electronic payment means. However, it is possible that a user may establish his right to a card in some manner other than by payment.

At present it will be assumed that the right to a card is obtained by payment. The general operational structure of the apparatus is shown in FIG. 4, which is similar to FIG. 1 of above-mentioned patent application No. 86 00 511. Reference can be made to this prior patent application for further details, with the reference numerals in present FIG. 4 corresponding to the reference numerals of FIG. 1 in the earlier patent application prefixed by the digit 2. Members 214 to 218 plus a return chute 222 are used for transactions in coin. Payment by means of bank notes is provided by means of a receptacle 222.

Preferably, payment may be made by conventional electronic payment means as illustrated at 223 ("smart" bank card, credit card, etc.).

This takes place under the control of a central control unit 212 which receives instructions from a user keyboard 224, and which actuates display means 226 and 228 as a result, for example to show the amount of money that remains to be paid and various other items of information.

After verifying the user's right to a card, the central unit 212 controls a dispense such as 230 or 232. given that a card magazine in accordance with the invention may contain a very large number of cards, it is presently believed that a single dispenser will suffice in practice.

The connections between the central unit 212 and the dispenser consist in:

controlling the position of the carrousel 110 (FIG. 2) or 300 (FIG. 5, described below);

actuating the electromagnet 159 and the stepper motor 145 for extracting a card unless the user has presented a card in the slot 105 for re-validation; and

simultaneously or sequentially positioning the programming unit 1, reversing the conveyors and actuating the electromagnet 139 until the new card has been dispesnsed to the user, and taking appropriate account of

the variations described above concerning incorrectly validated cards or cards for re-validation.

The programming unit itself has its motor **20** connected to the central unit **212** as well as its detectors **41, 42,** and **58,** and of course the set of tabs in the connector block **6.**

A variant magazine in accordance with the invention is now described with reference to FIGS. **5** and **5A.**

FIG. **5A** is a side view of the magazine itself constituted by a rigid disk-shaped container which is preferably closed by means of lead-sealed screws. Inside the container there is a flat disk **300** and drive means **320** coaxial therewith. The drive means **320** have associated control electronics inside the container **310** so as to make it impossible to rotate the disk **300** without knowing the details of the control means, and for example safety codes associated with control thereof.

FIG. **5** is a plan view of the disk **300** with the container **310** removed.

It can be seen that this disk carries a rack structure having a plurality of slots each of which houses a single card in a radial position such as **310-1, 310-2,** etc.

A card can be delivered only if its slot in the rack is level with the outlet slot **301** through the wall of the container, thereby allowing the card to drop through the slot.

The security obtained in this way is practically as good as that obtained in the first embodiment since the disk **300** cannot be rotated inside the container **310** without a thorough knowledge of the system and its drive security codes, or else without breaking the container **310.**

A card can then be taken up by a suitable mechanism for applying it to the path **140A** of the first conveyor.

Alternatively it may drop to a predetermined position in a slideway or chute which brings it into position between the wheels **131** and **132.** All of the wheels in the device can then be aligned.

It is important to ensure that theft of the card programming means will not enable cards to be fraudulently programmed. In order to make this possible, the equipment is advantageously permanently monitored over a telephone link. It then receives a coding key (e.g. a DES = Date Encryption Standard key as already used for inter-bank transactions, for example), with the key being required before cards can be validly programmed. Further, backed-up read/write memories may be automatically erased in the event of the device being broken into or stolen.

Further, the device in accordance with the invention may additionally include means for reading/writing the magnetic tracks of a card, with said means being located, for example, between the wheels **131** and **141.**

Naturally, the present invention is not limited to the embodiments described, but extends to any variant lying within the scope of the following claims.

I claim:

1. An automatic dispenser for microcircuit cards, said dispenser comprising:

a cabinet;

dispenser control means capable of dialog with a user, in order to verify the user's right to a card;

at least one magazine in the cabinet containing non-valid microcircuit cards;

pick-up means in the cabinet for extracting one card at a time from said magazine;

a programming unit in the cabinet having means for validating a non-valid microcircuit card and for re-validating a previously programmed microcircuit card;

first conveyor means for conveying the extracted non-valid card to said programming unit for validating said card;

second conveyor means for conveying an externally input and previously programmed card to said programming unit for re-validating said previously programmed card; and

third conveyor means for conveying the validated card or re-validated card from the programming unit to a card-dispensing slot through the wall of the cabinet.

2. A dispenser according to claim **1,** wherein the programming unit is also capable of verifying card validation, and wherein it includes means for rejecting any incorrectly-validated card and for storing it inside the cabinet.

3. A dispenser according to claim **1,** wherein said first and third conveyor means includes a common conveyor portion suitable for transferring the card to the programming unit and away therefrom.

4. A dispenser according to claim **3,** wherein the programming unit is movable and includes a second position in which it is no longer accessible to or from said common conveyor portion, thereby enabling invalid card rejection to take place directly from the common conveyor portion into an invalid card receptacle.

5. A dispenser according to claim **3,** wherein said pick-up means comprise a wheel mounted on a moving lever and suitable for cooperating on command with the magazine to extract the card therefrom and apply it to the first conveyor means.

6. A dispenser according to claim **3,** wherein the first conveyor means includes at least two pairs of wheels constituting said common portion, with at least one of said wheels being motor-driven.

7. A dispenser according to claim **3,** wherein the third conveyor means includes a belt passing in a closed loop between a first pair of wheels of the first conveyor means and between wheels and a last pair of wheels placed closed to the card-dispensing slot.

8. A dispenser according to claim **7,** wherein the intermediate pair of wheels of the third conveyor means also constitutes said pick-up means.

9. A dispenser according to claim **3,** wherein a card outlet from the magazine, the path along the first conveyor means, and a card inlet/outlet of the programming unit are substantially in alignment.

10. A dispenser according to claim **9,** wherein the path defined by the first pair and the last pair of wheels belonging to the third conveyor means is at a slope relative to the path through the first conveyor means, and wherein one of the first pair of wheels situated level with the transition between the conveyors is a moving wheel to enable a card to tilt without losing drive continuity.

11. A dispenser according to claim **10,** wherein the center of said moving wheel follows an arc of a circle which is substantially concentric with the other wheel of the same pair.

12. A dispenser according to claim **10,** including a card edge detector adjacent to said moving wheel, on the first conveyor side thereof.

13. A dispenser according to claim **3,** including a card edge detector situated close to the middle of the portion

specific to the third conveyor means, and a card edge detector close to the card dispensing slot.

14. A dispenser according to claim 1, wherein the card magazine includes at least one container housing a stack of cards which is resiliently-urged towards a pick-up position to enable said cards to be extracted therefrom.

15. A dispenser according to claim 14, wherein a plurality of such containers are mounted on a carrousel.

16. A dispenser according to claim 1, wherein the magazine comprises a carrousel having a card rack suitable for housing one card per rack slot, said carrousel being rotatably-mounted inside a disk-shaped container which is closed except for an outlet slot level with one of the card slots in the rack, said container also housing carrousel drive means.

17. A method for programming and dispensing microcircuit cards, comprising:

disposing inside a cabinet (a) at least one magazine containing non-valid microcircuit cards, (b) pick-up means for extracting one card at a time from said magazine, and (c) a programming unit for validating a non-valid microcircuit card and for re-validating a previously programming microcircuit card;

providing a dispenser control means capable of dialog with a user in order to verify the user's right to a card;

conveying a non-valid card extracted from the magazine to said programming unit for validating said non-valid card;

conveying an externally input and previously programmed card to said programming unit for re-validating said previously programmed card; and

conveying the validated card or the re-validated card to a card dispensing slot through the wall of the cabinet.

18. The method according to claim 17, including moving the programming unit to a position which is no longer accessible to or from conveyors from said validated or re-validated microcircuit cards for enabling invalid card rejection to take place directly from such conveyor into an invalid card receptacle contained within the cabinet.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 4,851,651

DATED : July 25, 1989

INVENTOR(S) : Michel M. Gaucher

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Specification:

Column 2, line 41, change "carrousel" to -- carousel --.
Column 2, line 55, change "carrousel" to -- carousel --.

Column 3, line 41, change "inventio" to -- invention --.

Column 4, line 1, change "abovementioned" to
-- above-mentioned --.
Column 4, line 7, change "round" to -- around --.
Column 4, line 24, change "tendin" to -- tending --.

Column 5, line 1, change "and" to -- the --.
Column 5, lines 4,5, delete "meanwhile".
Column 5, line 41, change "dispense" to -- dispenser --.
Column 5, lines 61,62, change "carrousel" to -- carousel --.

Column 6, line 1, change "if" to -- is --.
Column 6, line 54, change "dispense" to -- dispenser --.
Column 6, line 54, change "given" to -- Given --.
Column 6, line 60, change "carrousel" to -- carousel --.

Column 7, line 44, change "Date" to -- Data --.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 4,851,651

DATED : July 25, 1989

INVENTOR(S) : Michel M. Gaucher

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

Column 9, lines 9,11,12,16, change "carrousel" to -- carousel -- (all occurrences).

Signed and Sealed this

Twenty-seventh Day of November, 1990

Attest:

HARRY F. MANBECK, JR.

Attesting Officer

Commissioner of Patents and Trademarks